ESET MAIL SECURITY

PARA MICROSOFT EXCHANGE SERVER

Manual de instalação e Guia do usuário

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Clique aqui para fazer download da versão mais recente deste documento

ESET ENJOY SAFER TECHNOLOGY™

ESET **MAIL SECURITY**

Atendimento ao cliente: www.eset.com/support

REV. 21/10/2015

Índice

Índice

1. Introdução

O ESET Mail Security 6 para Microsoft Exchange Server é uma solução integrada que protege as caixas de correio contra vários tipos de conteúdo malicioso, incluindo anexos de email infectados por worms ou cavalos de troia, documentos que contêm scripts prejudiciais, esquemas de roubo de identidade e spam. O ESET Mail Security fornece três tipos de proteção: Antivírus, antispam e regras definidas pelo usuário. O ESET Mail Security filtra o conteúdo malicioso no nível do servidor de email, antes que ele chegue à caixa de entrada do cliente de email do destinatário.

O ESET Mail Security suporta o Microsoft Exchange Server versões 2003 e posteriores, bem como o Microsoft Exchange Server em um ambiente de agrupamento. Nas versões mais recentes (Microsoft Exchange Server 2003 e posteriores), também há suporte a funções específicas (caixa de correio, hub, edge). É possível gerenciar remotamente o ESET Mail Security em grandes redes com a ajuda do ESET Remote Administrator.

Enquanto fornece proteção ao Microsoft Exchange Server, o ESET Mail Security também inclui ferramentas para assegurar a proteção do próprio servidor (proteção residente, proteção do acesso à Web e proteção do cliente de email).

1.1 O que há de novo na versão 6?

- Gerente de quarentena de email - O administrador pode inspecionar objetos nessa seção de armazenamento e decidir se eles vão ser excluídos ou liberados. Este recurso oferece o gerenciamento simples de emails colocados em quarentena pelo agente de transporte.
- Interface web de quarentena de email - Uma alternativa baseada na web para o gerente de quarentena de email.
- Mecanismo antispam - Este componente essencial foi renovado e agora está sendo desenvolvido internamente.
- Rastreamento de banco de dados sob demanda - O rastreamento de banco de dados sob demanda usa o API EWS (Serviços da web do Exchange) para conectar ao Servidor do Microsoft Exchange via HTTP/HTTPS.
- Regras **-** O menu Regras permite aos administradores definir manualmente as condições de filtragem de email e as ações a serem tomadas com os emails filtrados. Regras da versão mais recente do ESET Mail Security foram refeitas do zero usando abordagem diferente.
- Agrupamento ESET - Similar ao ESET File Security 6 para Microsoft Windows Server, agrupas estação de trabalho em nós vão oferecer automação adicional ao gerenciamento devido a capacidade de distribuir uma política de configuração em todos os membros do agrupamento. A criação dos próprios agrupamentos é possível usando o nó instalado, que então pode instalar e iniciar todos os nós remotamente. Produtos de servidor da ESET são capazes de se comunicar uns com os outros e troquem dados como configurações e notificações, e podem sincronizar os dados necessários para a operação adequada de um grupo de instâncias do produto. Isso permite a mesma configuração do produto para todos os membros de um agrupamento. Agrupamento de Failover Windows e agrupamentos de Balanceamento de Carga de Rede (NLB) são compatíveis com ESET Mail Security. Além disso, é possível adicionar membros do Agrupamento ESET manualmente, sem a necessidade de um Agrupamento Windows específico. Agrupamentos ESET funcionam em ambientes de domínio e de grupo de trabalho.
- Rastreamento de armazenagem- Rastreia todos os arquivos compartilhados em um servidor local. Assim, fica fácil rastrear seletivamente apenas dados de usuário que estão armazenados no servidor de arquivos.
- Instalação baseada em componentes - você pode escolher quais componentes deseja adicionar ou remover.
- Exclusões de processos - exclui processos específicos do Rastreando de antivírus no acesso. Devido a função crítica de servidores dedicados (servidor de aplicativo, servidor de armazenamento, etc.) backups regulares são obrigatórios para garantir a recuperação oportuna de incidentes fatais de qualquer tipo. Para melhorar a velocidade de backup, integridade de processo e disponibilidade do serviço, algumas técnicas que sabe-se que entram em conflito com a proteção antivírus no nível de arquivo são usadas durante o backup. Problemas similares podem acontecer ao tentar migrações em tempo real de máquinas virtuais. A única forma eficiente de evitar ambas as situações é desativar o software antivírus. Ao excluir processos específicos (por exemplo, processos da solução de backup) todas as operações de arquivo que podem ser atribuídas a esses processos

excluídos são ignoradas e consideradas seguras, minimizando a interferência com o processo de backup. Recomendamos ter cuidado ao criar exclusões - uma ferramenta de backup que foi excluída pode acessar arquivos infectados sem acionar um alerta, que é o motivo pelo qual permissões estendidas só são permitidas no módulo de proteção em tempo real.

- Coletor de relatório ESET- Coleta automaticamente informações como ESET Mail Security configuração e vários relatórios. O Coletor de relatório ESET facilitará sua coleta das informações de diagnóstico necessárias para ajudar os técnicos da ESET a solucionar um problema rapidamente.
- eShell (ESET Shell) - O eShell 2.0 agora está disponível em ESET Mail Security. O eShell é uma interface de linha de comendo que oferece aos usuários avançados e administradores opções mais abrangentes para o gerenciamento de produtos do servidor da ESET.
- Rastreamento Hyper-V - É uma nova tecnologia que permite rastrear discos de Máquinas Virtuais (VM) em um Servidor Microsoft Hyper-V sem precisar de nenhum "Agente" na VM em particular.

1.2 Páginas de ajuda

Prezado(a) cliente, temos o prazer de dar as boas-vindas ao ESET Mail Security. Este guia é feito para ajudá-lo a usar ao máximo o ESET Mail Security.

Os tópicos neste guia são divididos em diversos capítulos e subcapítulos. Você pode encontrar as informações relevantes navegando pelo **Índice** das páginas de ajuda. Alternativamente, é possível usar o **Índice** para pesquisar por palavras-chave ou usar a **Pesquisa** no texto inteiro.

Para saber mais sobre qualquer janela no programa, pressione F1 no seu teclado enquanto a janela determinada está aberta. Será exibida a página de ajuda relacionada à janela que você está vendo.

o ESET Mail Security permite pesquisar tópicos de ajuda pela palavra-chave ou digitando palavras ou frases dentro do Guia do Usuário. A diferença entre os dois métodos é que a palavra-chave pode ser logicamente relacionada às páginas de ajuda que não contenham aquela palavra-chave no texto. Usando as palavras ou frases pesquisará o conteúdo de todas as páginas e exibirá somente aquelas contendo a palavra ou a frase pesquisada no texto real.

1.3 Métodos usados

Os métodos independentes a seguir são usados para rastrear emails:

- Proteção do banco de dados da caixa de entrada - conhecido anteriormente como Rastreamento da caixa de correio via VSAPI. Este tipo de proteção só está disponível para o Microsoft Exchange Server 2010, 2007 e 2003 operando na função Servidor Mailbox (Microsoft Exchange 2010 e 2007) ou Servidor Back-End (Microsoft Exchange 2003). Este tipo de rastreamento pode ser realizado em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que inclua a função de Mailbox ou Back-end).
- Proteção de transportador de email - conhecida anteriormente como Filtragem de mensagens no nível do servidor SMTP. Esta proteção é fornecida pelo agente de transporte e só está disponível para Microsoft Exchange Server 2007 ou mais recente operando na função de Servidor Edge Transport ou Servidor Hub Transport . Este tipo de rastreamento pode ser realizado em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que tenha uma das funções de servidor mencionadas).
- Rastreamento de banco de dados sob demanda - permite executar ou agendar um rastreamento do banco de dados de caixa de entrada Exchange. Este recurso só está disponível para Microsoft Exchange Server 2007 ou mais recente operando na função Servidor Mailbox ou Transporte de Hub. Isto também é aplicável em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que tenha uma das funções de servidor mencionadas). Veja funções do Exchange Server 2013 para detalhes específicos sobre funções no Exchange 2013.

1.3.1 Proteção do banco de dados da caixa de entrada

O processo de rastreamento das caixas de correio será disparado e controlado pelo Microsoft Exchange Server. Os emails no banco de dados de armazenamento do Microsoft Exchange Server serão rastreados continuamente. Dependendo da versão do Microsoft Exchange Server, da versão da interface VSAPI e das configurações definidas pelo usuário, o processo de rastreamento pode ser disparado em qualquer uma das seguintes situações:

- Quando o usuário acessa o email, por exemplo, em um cliente de email (o email é sempre rastreado com o banco de dados de assinatura de vírus mais recente)
- Em segundo plano, quando a utilização do Microsoft Exchange Server for menor
- Proativamente (com base no algoritmo interno do Microsoft Exchange Server)

A interface VSAPI atualmente é usada para rastreamento antivírus e proteção baseada em regras.

1.3.2 Proteção de transportador de email

A filtragem no nível do servidor SMTP é assegurada por um plugin especializado. No Microsoft Exchange Server 2000 e 2003, o plugin em questão (*Event Sink*) é registrado no servidor SMTP como parte do Internet Information Services (IIS). No Microsoft Exchange Server 2007/2010, o plugin está registrado como um agente de transporte nas funções *Edge* ou *Hub* do Microsoft Exchange Server.

A filtragem no nível do servidor SMTP por um agente de transporte fornece proteção sob a forma de antivírus, antispam e regras definidas pelo usuário. Ao contrário da filtragem de VSAPI, a filtragem no nível do servidor SMTP é executada antes que o email rastreado chegue à caixa de correio do Microsoft Exchange Server.

1.3.3 Rastreamento de banco de dados sob demanda

Como executar um rastreamento de banco de dados de email completo em ambientes de grande porte pode causar uma carga indesejada no sistema, você pode escolher quais bancos de dados e caixas de correio serão rastreados. Você pode filtrar os destinos de rastreamento ainda mais ao especificar o tempo das mensagens a rastrear, para minimizar o impacto nos recursos do sistema do servidor.

Os tipos de itens a seguir são rastreador tanto nas pastas Públicas quanto nas Caixas de entrada de usuários:

- Email
- Postar
- Itens de calendário (reuniões/compromissos)
- Tarefas
- Contatos
- Agenda

Você pode usar a lista suspensa para escolher as mensagens a serem rastreadas de acordo com sua marcação de hora. Por exemplo, mensagens modificadas na última semana. Você também pode escolher rastrear todas as mensagens, se necessário.

Selecione a caixa de seleção ao lado de **Rastrear corpos de mensagens** para ativar ou desativar a verificação do corpo da mensagem.

Clique em **Editar** para selecionar a pasta pública que será rastreada.

Rastreamento sob demanda do banco de dados

Rastrear mensagens modificadas na última semana

☑ Rastrear corpos de mensagens

Pastas públicas

Pastas públicas /tudo

Editar...

Caixas de correio

Servidores

Caixas de correio

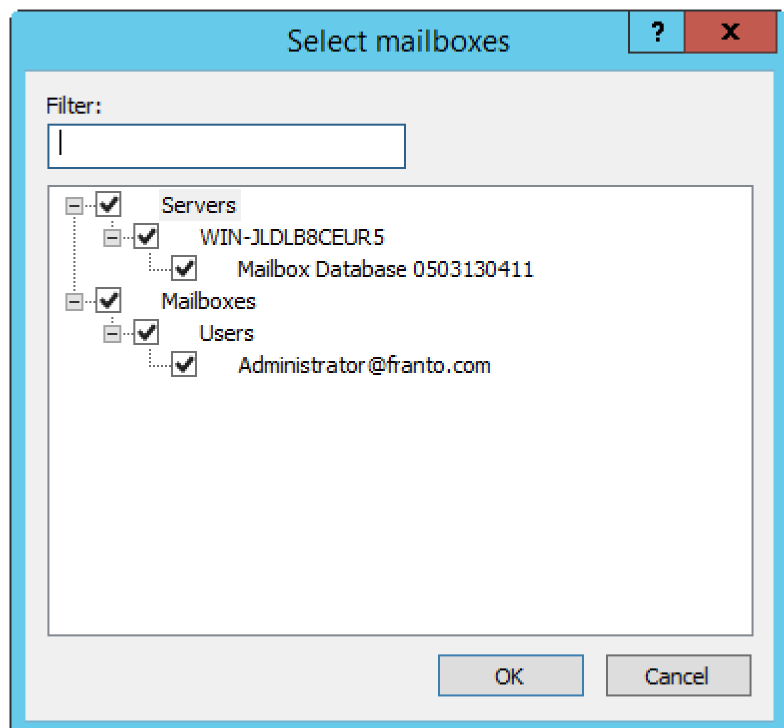
Editar...

Guardar

OK

Cancelar

Selecione as caixas de seleção ao lado dos Bancos de dados de servidor e caixas de entrada que você deseja rastrear. O **Filtro** permite que você encontre bancos de dados e caixas de entrada rapidamente, especialmente se houver um grande número de caixas de entrada em sua infraestrutura do Exchange.



Clique em **Salvar** para salvar seus destinos e parâmetros de rastreamento para o perfil de Rastreamento sob demanda.

1.4 Tipos de proteção

Há três tipos de proteção:

- Proteção antivírus
- Proteção antispam
- Aplicação de regras definidas pelo usuário

1.4.1 Proteção antivírus

A proteção antivírus é uma das funções básicas do ESET Mail Security. A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, e-mails e a comunicação pela Internet. Se uma ameaça com código malicioso for detectada, o módulo antivírus poderá eliminá-la, bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a Quarentena.

1.4.2 Proteção antispam

A proteção antispam integra várias tecnologias (RBL, DNSBL, Impressão digital, Verificação de reputação, Análise de conteúdo, Filtragem Bayesian, Regras, Listas manuais de permissões/proibições, etc.) para aumentar ao máximo a detecção de ameaças por email. O mecanismo de rastreamento antispam produz um valor de probabilidade na forma de uma porcentagem (0 a 100) para cada mensagem de email rastreada.

O ESET Mail Security também pode usar o método de Lista cinza (desativado por padrão) de filtragem de spam. O método baseia-se na especificação RFC 821, que determina que, como o SMTP é considerado um protocolo de transporte não confiável, todo MTA (Message Transfer Agent, Agente de Transferência de Mensagens) deve tentar repetidamente entregar um email após encontrar uma falha temporária na entrega. Muitas mensagens de spam são entregues uma vez a uma lista geral de endereços de email gerada automaticamente. A Lista cinza calcula um valor de controle (hash) para o endereço do remetente do envelope, o endereço do destinatário do envelope e o endereço IP do MTA remetente. Se o servidor não puder conseguir o valor de controle do trio em seu banco de

dados, ele se recusará a aceitar a mensagem, retornando um código de falha temporária (por exemplo, 451). Um servidor legítimo tentará entregar novamente a mensagem após um período variável. O valor de controle do trio será armazenado no banco de dados de conexões verificadas na segunda tentativa, permitindo que todos os emails com características relevantes sejam entregues desse momento em diante.

1.4.3 Aplicação de regras definidas pelo usuário

A proteção baseada em regras está disponível para rastreamento com a VSAPI e o agente de transporte. É possível usar a interface de usuário ESET Mail Security para criar regras individuais que também podem ser combinadas. Se uma regra usar várias condições, as condições serão vinculadas usando o operador lógico E. Consequentemente, a regra será executada somente se todas as suas condições forem cumpridas. Se várias regras forem criadas, o operador lógico OU será aplicado, o que significa que o programa executará a primeira regra para a qual as condições forem atendidas.

Na sequência de rastreamento, a primeira técnica usada é a lista cinza – se estiver ativada. Os procedimentos consequentes sempre executarão as seguintes técnicas: proteção com base em regras definidas pelo usuário, seguida de um rastreamento antivírus e, por último, um rastreamento antispam.

1.5 Interface do usuário

o ESET Mail Security tem uma interface gráfica de usuário (GUI) projetada para ser o mais intuitiva possível. A GUI permite que os usuários acessem rápida e facilmente as principais funções do programa.

Além da interface gráfica do usuário principal, há uma **janela de configuração avançada** acessível em qualquer local do programa, pressionando a tecla F5.

Na janela de Configuração avançada, você pode configurar os ajustes e opções com base em suas necessidades. O menu da esquerda é composto das categorias a seguir: . Algumas das categorias principais contém subcategorias. Ao clicar em um item (categoria ou subcategoria) no menu da esquerda, as respectivas configurações daquele item são exibidas no painel da direita.

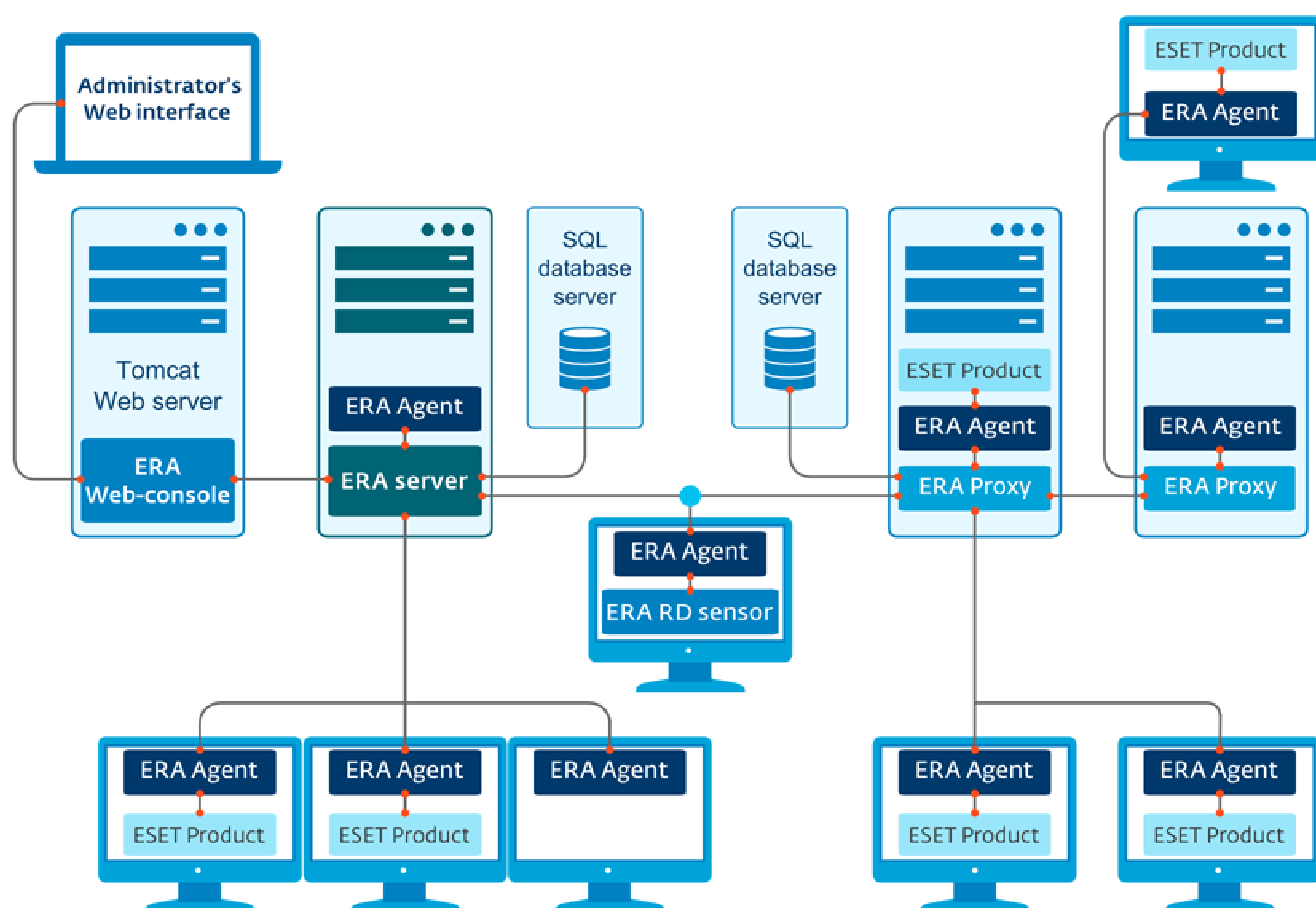
Para obter informações mais detalhadas sobre a interface gráfica do usuário, clique aqui.

1.6 Gerenciado via ESET Remote Administrator

ESET Remote Administrator (ERA) é um aplicativo que permite que você gerencie produtos ESET em um ambiente em rede a partir de um local central. O sistema de gerenciamento de tarefas do ESET Remote Administrator permite que você instale soluções de segurança da ESET em computadores remotos e responda rapidamente a novos problemas e ameaças. O ESET Remote Administrator não fornece proteção contra código malicioso por si só, ele conta com a presença de uma solução de segurança da ESET em cada cliente.

As soluções de segurança da ESET são compatíveis com redes que incluem vários tipos de plataforma. Sua rede pode incluir uma combinação de sistemas operacionais Microsoft, Linux e OS X que são executados em dispositivos móveis (celulares e tablets).

A imagem a seguir mostra uma arquitetura de exemplo para uma rede protegida por soluções de segurança da ESET gerenciada por ERA:



i **OBSERVAÇÃO:** Para obter mais informações sobre o ERA, consulte ESET Remote AdministratorAjuda on-line.

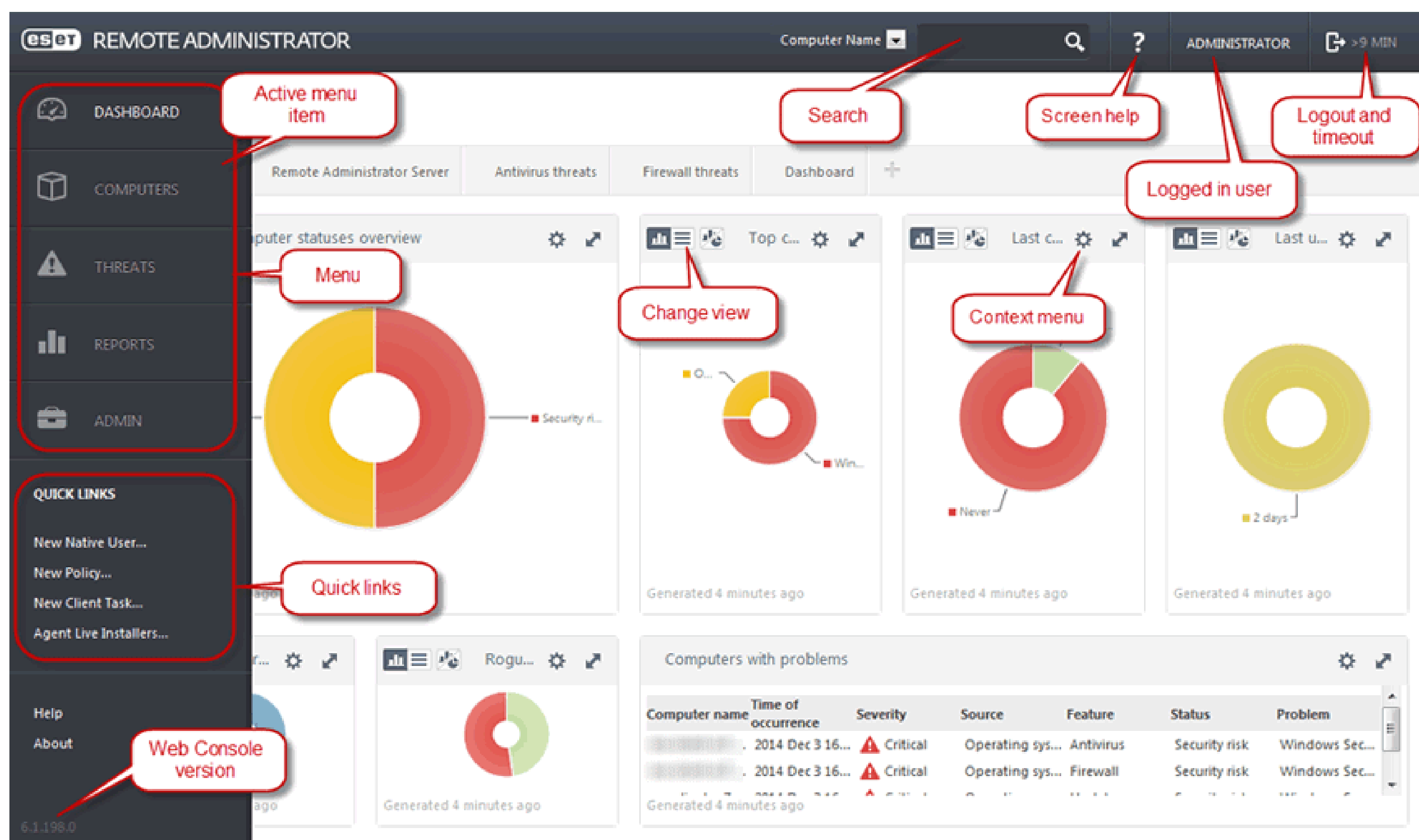
1.6.1 Servidor ERA

ESET Remote Administrator Server é um componente primário do ESET Remote Administrator. Ele é o aplicativo executivo que processa todos os dados recebidos de clientes que se conectam ao Servidor (por meio do Agente ERA). O Agente ERA facilita a comunicação entre o cliente e o servidor. Dados (relatórios de cliente, configuração, replicação do agente, etc.) são armazenados em um banco de dados. Para processar dados corretamente, o Servidor ERA exige uma conexão estável com um servidor de banco de dados. Recomendamos que você instale o Servidor ERA e seu banco de dados em servidores separados para otimizar o desempenho. A máquina na qual o Servidor ERA está instalado deve ser configurada para aceitar todas as conexões de Agente/Proxy/RD Sensor, que são verificadas usando certificados. Quando o Servidor ERA estiver instalado, você pode abrir o Console da Web ERA que se conecta aos Servidor ERA (como exibido no diagrama). A partir do console da Web, todas as operações do Servidor ERA são realizadas enquanto se gerencia as soluções de segurança ESET dentro da sua rede.

1.6.2 Console da web

O **console da Web ERA** é uma interface de usuário na Web que apresenta dados do Servidor ERA e permite que você gerencie as soluções de segurança da ESET em seu ambiente. O Console da Web pode ser acessado usando um navegador. Ele exibe uma visão geral do status de clientes em sua rede e pode ser usado para implantar remotamente soluções da ESET em computadores não gerenciados. Se você decidir tornar o servidor Web acessível a partir da internet, você terá a vantagem de poder usar o ESET Remote Administrator a partir de praticamente qualquer lugar e qualquer dispositivo com uma conexão ativa com a Internet.

Este é o Painel do console da Web:



Dentro da barra superior do console da Web está a ferramenta de **Pesquisa rápida**. Selecione **Nome do computador**, **Endereço IPv4/IPv6** ou **Nome da ameaça** no menu suspenso, digite sua sequência de pesquisa no campo de texto e clique no símbolo da lente de aumento ou pressione **Enter** para pesquisar. Você será redirecionado para a seção Grupos, na qual sua pesquisa será exibida - como um cliente ou uma lista de clientes. Todos os clientes são gerenciados através do console da web. Você pode acessar o console da web usando os dispositivos e navegadores mais comuns.

OBSERVAÇÃO: Para obter mais informações consulte ESET Remote Administrator Ajuda on-line.

1.6.3 Agente

O **Agente ERA** é uma parte essencial do produto ESET Remote Administrator. Um produto ESET em uma máquina do cliente (por exemplo ESET Endpoint Security for Windows) comunica-se com o Servidor ERA exclusivamente por meio do Agente. Esta comunicação permite o gerenciamento dos produtos ESET em todos os clientes remotos a partir de um local central. O Agente coleta informações do cliente e as envia para o Servidor. E se o Servidor enviar uma tarefa para o cliente, a tarefa é enviada para o Agente e o Agente enviará essa tarefa para o cliente. Toda a comunicação em rede ocorre entre o Agente e a parte superior da rede do ERA: Servidor e Proxy.

O Agente ESET usa um dos seguintes três métodos para se conectar ao Servidor:

1. O Agente do Cliente é diretamente conectado ao Servidor.
2. O Agente do Cliente é conectado através de um Proxy, que é conectado ao Servidor.
3. O Agente do Cliente é conectado ao Servidor através de vários Proxies.

O Agente ESET comunica-se com soluções da ESET instaladas em um cliente, coleta informações de programas nesse cliente e transmite as informações de configuração recebidas do Servidor para o cliente.

OBSERVAÇÃO: O proxy da ESET tem seu próprio Agente, que processa todas as tarefas de comunicação entre clientes, outros proxies e o Servidor.

1.6.4 RD Sensor

O **RD (Rogue Detection) Sensor** é uma ferramenta de pesquisa para computadores na rede. O RD Sensor faz parte do ESET Remote Administrator e foi desenvolvido para detectar máquinas em sua rede. Ele oferece uma forma conveniente de adicionar novos computadores ao ESET Remote Administrator sem a necessidade de adicioná-los manualmente. Todo computador detectado em sua rede é exibido no console da Web. A partir daí, é possível realizar ações adicionais com computadores cliente individuais.

O RD Sensor consiste em um mecanismo de escuta passivo que detecta computadores que estão presentes na rede e envia informações sobre eles para o Servidor ERA. O Servidor ERA então avalia se os PCs detectados na rede são desconhecidos para o servidor ERA ou se já são gerenciados.

1.6.5 Proxy

Proxy ERA é outro componente do ESET Remote Administrator e atende a duas finalidades. Em uma rede de médio porte ou corporativa com muitos clientes (por exemplo, 10.000 clientes ou mais), você pode usar o Proxy ERA para distribuir a carga entre vários Proxies ERA, facilitando para o Servidor ERA principal. A outra vantagem do Proxy ERA é que você pode usá-lo ao se conectar a uma filial remota com um link fraco. Isso significa que o Agente ERA em cada cliente não está conectando ao Servidor ERA principal diretamente através do Proxy ERA, que está na mesma rede local da filial. Isso libera o link da filial. O Proxy ERA aceita conexões de todos os Agentes ERA, soma seus dados e atualiza os dados para o Servidor ERA principal (ou a outro Proxy ERA). Isso permite que sua rede acomode mais clientes sem comprometer o desempenho de suas consultas de banco de dados e rede.

Dependendo da configuração de sua rede, é possível que um Proxy ERA se conecte a outro Proxy ERA e então se conecte ao Servidor ERA principal.

Para o funcionamento correto do Proxy ERA, o computador host no qual você instalará o Proxy ERA deverá ter um Agente da ESET instalado e deve estar conectado ao nível superior (seja Servidor ERA ou Proxy ERA superior, se houver um) de sua rede.

OBSERVAÇÃO: Para um exemplo do cenário de implementação do Proxy ERA, consulte a ESET Remote Administrator Ajuda on-line.

2. Requisitos do sistema

Sistemas operacionais compatíveis:

- Microsoft Windows Server 2003 (x86 e x64)
- Microsoft Windows Server 2003 R2 (x86 e x64)
- Microsoft Windows Server 2008 (x86 e x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Versões compatíveis do Microsoft Exchange Server:

- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU4 (SP1), CU5, CU6, CU7, CU8
- Microsoft Exchange Server 2016

Os requisitos de hardware dependem da versão do sistema operacional em uso. Recomendamos ler a documentação do Microsoft Windows Server para obter informações mais detalhadas sobre os requisitos de hardware.

3. Instalação

Após comprar o ESET Mail Security, o instalador pode ser transferido do site da ESET (www.eset.com) em um pacote .msi.

Observe que você precisa executar o instalador na conta do Administrador incorporado. Qualquer outro usuário, apesar de ser membro do grupo de administradores, não terá direitos de acesso suficientes. Portanto, é necessário usar a conta de administrador incorporado, pois você não poderá concluir a instalação com êxito em qualquer outra conta de usuário que não seja Administrador.

Há duas maneiras de executar o instalador:

- Você pode fazer login localmente usando as credenciais de conta do Administrador e simplesmente ao executar o instalador
- Você pode se conectar como outro usuário, mas precisa abrir o aviso de comando com Executar como... e digitar as credenciais de conta de Administrador para ter o cmd executando como Administrador e então digitar o comando para executar o instalador (p. ex., msiexec /i mas você precisa substituir pelo nome de arquivo exato do instalador msi que você baixou)

Inicie o instalador e aceite o Acordo de licença para o usuário final (EULA), e o assistente de instalação o guiará pela configuração. Se você escolher não aceitar os termos no Acordo de licença, o assistente não continuará.

Completo
Este é o tipo de instalação recomendado. Instalará todos os recursos do ESET Mail Security. Depois de escolher este tipo de instalação, será preciso apenas especificar as pastas onde instalar o produto, mas é possível apenas aceitar as pastas de instalação padrão predefinidas. O instalador instala todos os recursos do programa automaticamente.

Personalizar
Com o tipo de instalação personalizada é possível escolher quais recursos do programa do ESET Mail Security serão instalados no seu sistema. Você verá uma lista típica de recursos/componentes dos quais selecionar para a instalação.

Além da instalação com o assistente, é possível escolher instalar o ESET Mail Security silenciosamente através da linha de comando. Este tipo de instalação não requer nenhuma interação como quando se usa o assistente, da forma descrita acima. Ele é útil, por exemplo, para automação ou aprimoramento. Este tipo de instalação também é chamado de desacompanhado, já que ele não precisa de nenhuma ação do usuário.

Instalação silenciosa/desacompanhada
Instalação completa através da linha de comando: `msiexec /i <packagename> /qn /l*xv msi.log`

i **OBSERVAÇÃO**: Recomendamos que instale o ESET Mail Security em um SO instalado e configurado recentemente, se possível. No entanto, se precisar instalá-lo em um sistema existente, o melhor a fazer é desinstalar a versão anterior do ESET Mail Security, reiniciar o servidor e instalar o novo ESET Mail Security em seguida.

i **OBSERVAÇÃO**: Se você já usou outro software antivírus de terceiros antes no seu sistema, recomendamos desinstalar o outro software completamente antes da instalação do ESET Mail Security. Para isso, você pode usar o ESET AV Remover, que facilita a desinstalação.

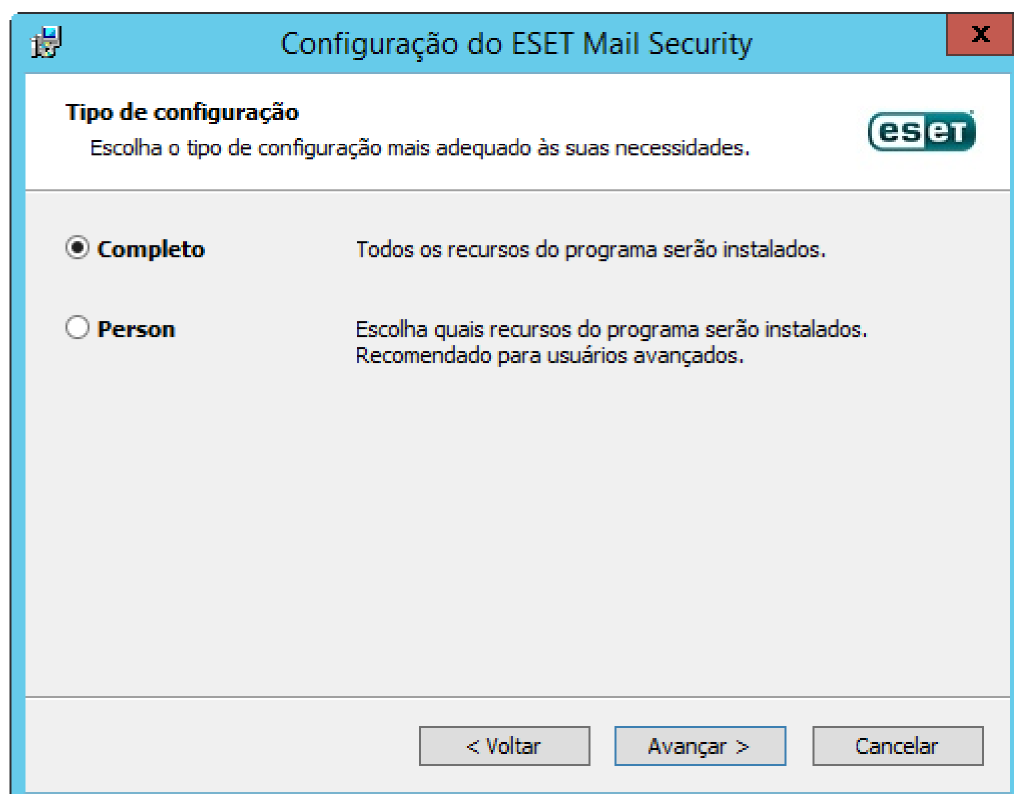
3.1 Etapas de instalação do ESET Mail Security

Siga as etapas abaixo para instalar o ESET Mail Security usando o Assistente de instalação:



Depois de aceitar o EULA, selecione um dos seguintes tipos de instalação:

- **Completo** - Instalar todos os recursos do ESET Mail Security. Este é o tipo de instalação recomendado.
- **Personalizado** - Selecione quais recursos do ESET Mail Security serão instalados em seu sistema.



Instalação completa:

Também chamada de instalação completa. Isto vai instalar todos os componentes do ESET Mail Security. Você será

solicitado a selecionar o local onde o ESET Mail Security será instalado. Por padrão, o programa é instalado em C:\Program Files\ESET\ESET Mail Security. Clique em **Procurar** para alterar esses locais (não recomendado).



Instalação personalizada:

Deixa você escolher quais recursos deseja instalar. Útil quando deseja personalizar seu ESET Mail Security para ter apenas os componentes que você precisa.



Você pode adicionar ou remover componentes incluídos na sua instalação. Para isso, execute o pacote de instalador .msi usado durante a instalação inicial ou vá para **Programas e recursos** (pode ser acessado no Painel de Controle do Windows), clique com o botão direito em ESET Mail Security e selecione **Alterar**. Siga as etapas abaixo para adicionar ou remover componentes.

Processo de Modificação de componente (Adicionar/remover), Reparar e Remover:

Existem 3 opções disponíveis. É possível **Modificar** os componentes instalados, **Reparar** sua instalação do ESET Mail Security ou **Remover**(desinstalar) completamente.



Se escolher **Modificar**, uma lista de todos os componentes disponíveis do programa é exibida. Escolha os componentes que deseja adicionar ou remover. É possível adicionar/remover vários componentes ao mesmo tempo. Clique no componente e selecione uma opção no menu suspenso:



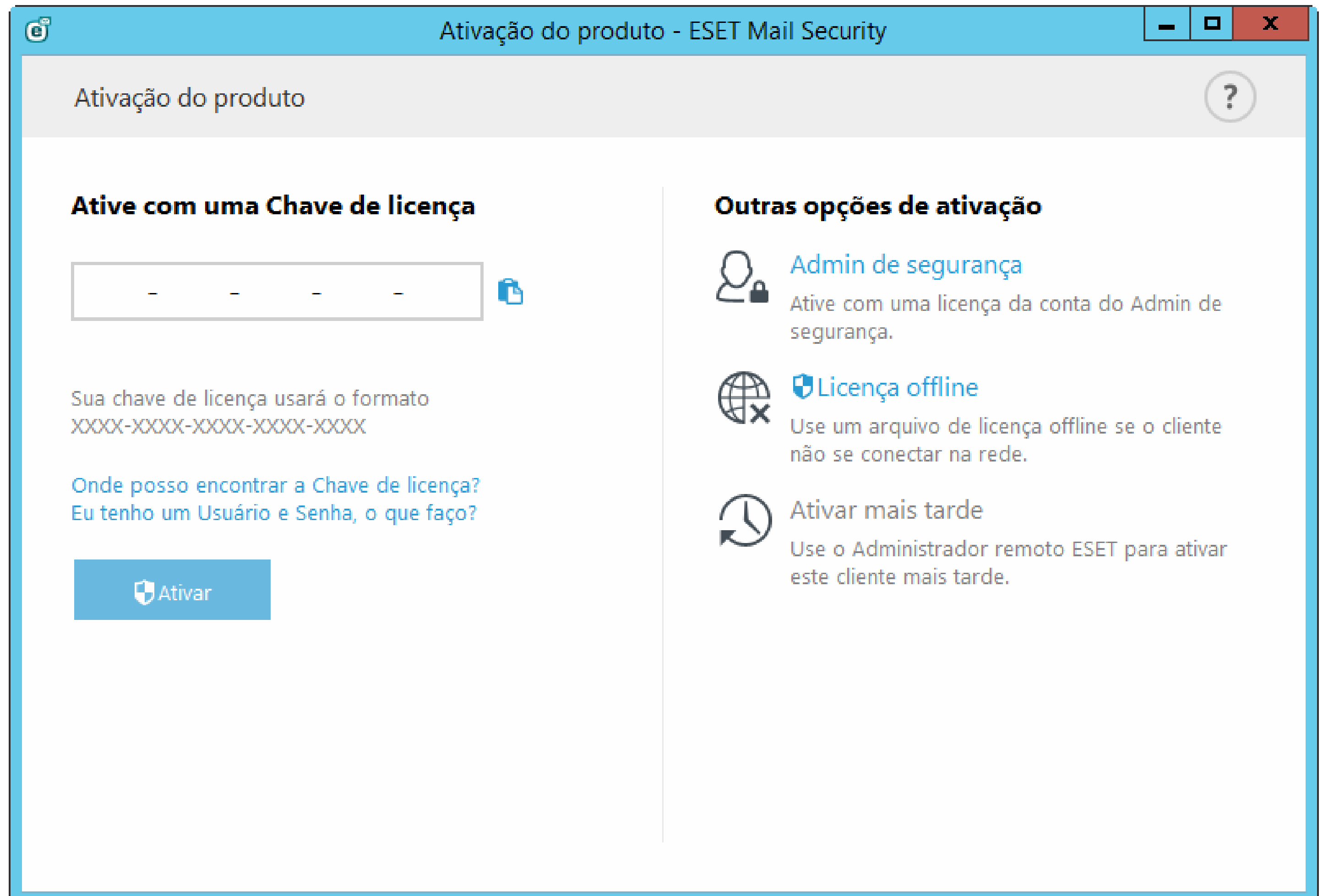
Ao selecionar uma opção, clique em **Modificar** para realizar as modificações.

OBSERVAÇÃO: Você pode modificar os componentes instalados a qualquer momento ao executar o instalador. Para a maioria dos componentes, a reinicialização do servidor não é necessária para realizar a mudança. A interface

gráfica do usuário vai reiniciar e você verá somente os componentes que escolheu instalar. Para componentes que requerem a reinicialização do servidor, o Windows Installer irá solicitar que você reinicie e os novos componentes estarão disponíveis assim que o servidor estiver online novamente.

3.2 Ativação do produto

Depois da conclusão da instalação, você será solicitado a ativar o produto.



Selecione um dos métodos disponíveis para ativar o ESET Mail Security. Para obter mais informações, consulte Como ativar o ESET Mail Security.

Depois de ter ativado o ESET Mail Security com êxito, a janela principal do programa será aberta e exibirá seu status atual na página de Monitoramento.

A janela principal do programa também exibirá notificações sobre outros itens, como atualizações do sistema (Atualizações do Windows) ou atualizações do banco de dados de assinatura de vírus. Quando todos os itens que precisam de atenção forem solucionados, o status de monitoramento ficará verde e exibirá o status "**Proteção máxima**".

3.3 Servidor de terminal

Se você estiver instalando o ESET Mail Security em um Windows Server que atue como Servidor de terminal, você pode desejar desativar a interface gráfica do usuário do ESET Mail Security para evitar que ela inicie todas as vezes em que um usuário fizer login. Consulte Desativar a interface gráfica do usuário no servidor de terminal para conhecer as etapas específicas para desativá-la.

3.4 ESET AV Remover

Para remover/desinstalar software antivírus de terceiros de seu sistema, recomendados usar o ESET AV Remover. Para fazer isso, siga as etapas:

1. Fazer download do ESET AV Remover do site da ESET página de download de Acessórios.
2. Clique em **Eu aceito, iniciar pesquisa** para aceitar o EULA e iniciar a pesquisa no seu sistema.
3. Clique em **Iniciar desinstalador** para remover o software antivírus instalado.

Para uma lista de software antivírus de terceiros que podem ser removidos usando o ESET AV Remover, consulte este artigo da base de conhecimento.

3.5 Atualização para uma versão mais recente

Versões mais recentes do ESET Mail Security são lançadas para fornecer aprimoramentos ou corrigir problemas que não podem ser resolvidos por meio de atualizações automáticas dos módulos do programa. É possível realizar uma atualização a partir de versões mais antigas do ESET Mail Security (4.5 e anteriores), embora seja uma atualização para uma arquitetura diferente. Há duas maneiras de atualizar para uma versão mais recente:

- Manualmente, por meio de download e instalação de uma versão mais recente sobre sua versão existente. Basta executar o instalador e realizar a instalação como de costume, o ESET Mail Security vai transferir sua configuração existente automaticamente, com algumas exceções (veja a observação abaixo).
- Remotamente, em um ambiente de rede, usando o ESET Remote Administrator.

Importante: Existem algumas exceções durante a atualização, nem todas as suas configurações serão preservadas, especialmente as Regras. Isto acontece porque a funcionalidade das Regras foi totalmente refeita no ESET Mail Security 6 usando uma abordagem diferente. Regras das versões anteriores do ESET Mail Security não são compatíveis com regras no ESET Mail Security versão 6. Recomendamos configurar a Regras manualmente, isso deverá ajudá-lo.

A seguir está uma lista de configurações que são preservadas de versões anteriores do ESET Mail Security:

- Configuração gera do ESET Mail Security.
- Configurações de proteção antispam:
  - Todas as configurações das versões anteriores serão idênticas, novas configurações usarão o valor padrão.
  - Lista de permissões e lista de proibições.

OBSERVAÇÃO: Assim que você tiver atualizado o ESET Mail Security, recomendamos revisar todas as configurações para verificar se elas estão configuradas corretamente e de acordo com suas necessidades.

3.6 Funções do Exchange Server - Edge versus Hub

Os servidores Edge Transport e Hub Transport têm recursos antispam desativados por padrão. Esta é a configuração desejada em uma organização Exchange com um servidor Edge Transport. Recomenda-se ter o servidor de Transporte de Edge executando o antispam do ESET Mail Security configurado para filtrar mensagens antes de elas serem roteadas para a organização com Exchange.

A função de Edge é o local preferido para rastreamento antispam, pois permite que o ESET Mail Security rejeite spam no início do processo, sem exercer uma carga desnecessária nas camadas da rede. Ao usar esta configuração, as mensagens de entrada são filtradas pelo ESET Mail Security no servidor de Transporte Edge, para que possam ser movidas com segurança para o servidor de Transporte Hub sem a necessidade de filtragem adicional.

Se sua organização não usa o servidor Edge Transport e tem somente o servidor Hub Transport, recomendamos a ativação dos recursos antispam no servidor de Hub Transport que recebem mensagens de entrada da Internet via SMTP.

3.7 Funções do Exchange Server 2013

A arquitetura do Exchange Server 2013 é diferente das versões anteriores do Microsoft Exchange. Desde a introdução do Exchange 2013, CU4 (que é na verdade SP1 para o Exchange 2013) reintroduziu a função de servidor de Edge Transport.

Se você estiver planejando proteger o Microsoft Exchange 2013 com o ESET Mail Security, certifique-se de instalar o ESET Mail Security em um sistema executando o Microsoft Exchange 2013 com a função do servidor Mailbox ou Edge Transport.

A exceção é se você estiver planejando instalar o ESET Mail Security no Windows SBS (Small Business Server) ou ter o Microsoft Exchange 2013 com várias funções em um único servidor. Nesse caso, todas as funções do Exchange estão sendo executadas no mesmo servidor, portanto o ESET Mail Security fornecerá proteção completa, inclusive proteção de servidores de email.

Se você instalar o ESET Mail Security em um sistema executando apenas a função de servidor Client Access (servidor CAS dedicado), os recursos mais importantes do ESET Mail Security serão desativados, especialmente os recursos de servidor de email. Nesse caso, apenas a proteção em tempo real do sistema de arquivos e alguns componentes que pertencem a Proteção do computador estarão funcionando, portanto servidores de email não estarão protegidos. Por isso, não recomendamos instalar o ESET Mail Security em um servidor com função de servidor de Client Access. Isso não se aplica ao Windows SBS (Small Business Server) e Microsoft Exchange com várias funções no mesmo computador, conforme mencionado acima.

i **OBSERVAÇÃO**: Devido a restrições técnicas do Microsoft Exchange 2013, o ESET Mail Security não é compatível com a função do servidor Client Access (CAS). Isso não se aplica ao Windows SBS ou Microsoft Exchange 2013 instalado em um único servidor com todas as funções de servidor - neste caso, você pode executar o ESET Mail Security com a função CAS no servidor, já que o servidor Mailbox e o servidor Edge Transport estão protegidos.

3.8 Conector POP3 e antispam

O Microsoft Windows versão Small Business Server (SBS) contém um Conector POP3 nativo integrado que permite que o servidor busque emails de servidores POP3 externos. A implementação deste Conector POP3 Microsoft nativo difere de uma versão SBS para outra.

o ESET Mail Security é compatível com o Microsoft SBS Conector POP3, se for configurado corretamente. As mensagens obtidas por download via o Microsoft Conector POP3 são rastreadas quanto à presença de spam. A proteção antispam para essas mensagens é possível porque o Conector POP3 encaminha as mensagens de email de uma conta POP3 para o Microsoft Exchange Server via SMTP.

ESET Mail Security foi testado com serviços de email populares, como **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** e **gmx.de** nos sistemas SBS a seguir:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

Importante: Se estiver usando um Microsoft SBS Conector POP3 integrado e tiver todas as mensagens de email rastreadas para spam, vá para a Configuração avançada, navegue até **Servidor** > **Proteção de transportador de email** > Configurações avançadas e para **Rastrear também as mensagens recebidas das conexões autenticadas ou internas** selecione **Rastrear usando a proteção antivírus e antispam** na lista suspensa. Isso garante a proteção antispam para emails buscados de contas POP3.

Você também pode usar um conector POP3 de terceiros como P3SS (em vez do Microsoft SBS Conector POP3 integrado). O ESET Mail Security foi testado nos seguintes sistemas (usando o conector P3SS buscando mensagens do **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** e **gmx.de**):

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 com Exchange Server 2007
- Microsoft Windows Server 2008 R2 com Exchange Server 2010
- Microsoft Windows Server 2012 R2 com Exchange Server 2013

4. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET Mail Security, as partes principais do menu, funcionalidade e configurações básicas.

4.1 A interface do usuário

A janela principal do ESET Mail Security é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

As seções diferentes do menu principal são descritas abaixo:

Monitoramento - Fornece informações sobre o status da proteção do ESET Mail Security, validade da licença, atualização mais recente do banco de dados de assinatura de vírus, estatísticas básicas e informações do sistema.

Relatórios - Acesse os relatórios com informações sobre todos os eventos importantes do programa que ocorreram. Estes arquivos oferecem uma visão geral de ameaças detectadas, assim como outros eventos de segurança relacionados.

Rastrear - Permite que você configure e inicie um Rastreamento de armazenagem, Rastreamento inteligente, Rastreamento personalizado ou Rastreamento de mídia removível. Você também pode repetir o último rastreamento que foi executado.

Atualizar - Exibe informações sobre o banco de dados de assinatura de vírus e notifica se uma atualização estiver disponível. A ativação do produto também pode ser realizada a partir desta seção.

Configuração - Aqui é possível ajustar as configurações de segurança do seu Servidor e Computador.

Ferramentas- Fornece informações adicionais sobre seus sistema e proteção, além de ferramentas que ajudam a gerenciar ainda mais sua segurança. A seção Ferramentas contém os itens a seguir: Processos em execução, Monitorar atividade, Coletor de Relatório ESET, Estatísticas da proteção, Agrupamento, ESET Shell, ESET SysInspector, ESET SysRescue Live para criar um CD ou USB de restauração e uma Agenda. Você também pode Enviar uma amostra para análise e verificar sua Quarentena.

Ajuda e suporte - Fornece acesso a arquivos de ajuda, base de conhecimento da ESET e outras ferramentas de suporte. Além disso, estão disponíveis links para abrir uma solicitação de suporte do Atendimento ao cliente e informações sobre ativação do produto.

A tela **Status da proteção** informa sobre o nível de proteção atual do seu computador. O ícone verde de status da **Proteção máxima** indica que a proteção máxima está garantida.

A janela de status também exibe os links rápidos para recursos mais usados do ESET Mail Security e informações sobre a última atualização.

eset MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

MONITORAMENTO
RELATÓRIOS
RASTREAR
QUARENTENA DE EMAIL
ATUALIZAR
CONFIGURAÇÃO
FERRAMENTAS
AJUDA E SUPORTE

ENJOY SAFER TECHNOLOGY™

Proteção máxima

Licença
Válido até: 12/31/2016

O banco de dados de assinatura de vírus está atualizado
Última atualização: 8/26/2015 9:51:23 AM

Estatísticas de proteção do sistema de arquivos

Infectado:	0
Limpo:	0
Limpar:	8430
Total::	8430

Versão do produto	6.2.10009.1
Nome de servidor	WIN-JLDLB8CEUR5.franto.com
Sistema	Windows Server 2012 R2 Standard 64-bit (6.3.9600)
Computador	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2600 MHz), 12288 MB RAM
Tempo de ativação do servidor	18 minutos
Contagem da caixa de entrada	11 domínio, 11 local

O que fazer se o programa não funcionar adequadamente?

Módulos que estão funcionando adequadamente recebem um ícone de marcação verde. Módulos que não são totalmente funcionais recebem um ponto de exclamação vermelho ou um ícone de notificação laranja. Informações adicionais sobre o módulo serão mostradas na parte superior da janela. Uma solução sugerida para corrigir o módulo também é exibida. Para alterar o status de módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.

O ícone vermelho indica problemas críticos - a proteção máxima do seu computador não está garantida. Este status é exibido quando:

- **Proteção antivírus e antispyware desativada** - Você pode reativar a proteção antivírus e antispyware clicando em **Ativar proteção em tempo real** no painel **Status da proteção** ou no painel **Ativar proteção antivírus e antispyware** no painel **Configuração** na janela principal do programa.
- Você está usando um banco de dados de assinatura de vírus desatualizado.
- O produto não está ativado.
- **Sua licença está expirada** - Isso é indicado pelo ícone do status da proteção que fica vermelho. O programa não pode ser atualizado após a licença expirar. Recomendamos que você siga as instruções da janela de alerta para renovar sua licença.

O ícone laranja indica que seu produto ESET requer atenção devido a um problema não crítico. As possíveis razões são:

- **A proteção do acesso à web está desativada** - Você pode reativar a proteção do acesso à web clicando na notificação de segurança e em **Ativar proteção do acesso à web**.

- **Sua licença expirará em breve** - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação. Depois que a licença expirar, o programa não poderá ser atualizado e o ícone do status da proteção

ficará vermelho.

Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na Base de conhecimento da ESET. Se ainda precisar de ajuda, envie uma solicitação de suporte ao Atendimento ao cliente da ESET. O Atendimento ao Cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a encontrar uma solução.

Para visualizar seu **Status da proteção**, clique na opção superior no menu principal. Um resumo de status sobre o funcionamento do ESET Mail Security será exibido na janela primária, e será exibido um submenu com duas opções: **Monitorar atividade** e **Estatísticas**. Selecione uma das opções para visualizar informações mais detalhadas sobre o sistema.

Quando o ESET Mail Security é executado em sua funcionalidade completa, o ícone de **Status da proteção** aparece em verde. Quando a atenção é solicitada, ele aparece em laranja ou vermelho.

Clique em **Monitorar atividade** para ver um gráfico em tempo real da atividade do sistema de arquivos (eixo horizontal). O eixo vertical exibe a quantidade de dados lidos (linha azul) e de dados gravados (linha vermelha).

O submenu **Estatísticas** possibilita ver a quantidade de objetos infectados e limpos de um módulo em particular. Há vários módulos dos quais você pode escolher, selecionando-os na lista suspensa.

4.2 Relatórios

Os relatórios contêm informações sobre os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. Relatórios são essenciais na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em relatório realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações do detalhamento do relatório. É possível visualizar mensagens de texto e relatórios diretamente do ambiente do ESET Mail Security ou exportá-las para exibição em outro lugar.

Os relatórios podem ser acessados na janela principal do programa, clicando em **Arquivos de relatório**. Selecione o tipo de relatório desejado no menu suspenso. Os seguintes relatórios estão disponíveis:

- **Ameaças detectadas** - O relatório de ameaças fornece informações detalhadas sobre as infiltrações detectadas pelos módulos do ESET Mail Security. Isso inclui a hora da detecção, nome da ameaça, local, ação realizada e o nome do usuário conectado no momento em que a ameaça foi detectada. Clique duas vezes em qualquer entrada de relatório para exibir seus detalhes em uma janela separada.
- **Eventos** - Todas as ações importantes executadas pelo ESET Mail Security são registradas no relatório de eventos. O relatório de eventos contém informações sobre eventos e erros que ocorreram no programa. Essa opção foi desenvolvida para ajudar administradores do sistema e usuários na solução de problemas. Com frequência, informações encontradas aqui podem ajudá-lo a encontrar uma solução para o problema ocorrido no programa.
- **Rastrear o computador** - Todos os resultados de rastreamento são exibidos nesta janela. Cada linha corresponde a um rastreamento no computador. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo rastreamento.
- **HIPS** - Contém registros de regras específicas que foram marcadas para registro. O protocolo exibe o aplicativo que acionou a operação, o resultado (se a regra foi permitida ou proibida) e o nome da regra criada.
- **Sites filtrados** - Uma lista de sites que foram bloqueados pela Proteção do acesso à web. Nesses relatórios, você poderá ver o horário, URL, usuário e aplicativo que criaram uma conexão para o site específico.
- **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com a respectiva regra de controle de dispositivo serão registrados no relatório. Se a regra não coincidir com um dispositivo conectado, uma entrada de relatório para um dispositivo conectado não será criada. Aqui, você também pode visualizar detalhes, como tipo de dispositivo, número de série, nome do fornecedor e tamanho da mídia (se disponível).
- **Rastreamento de banco de dados** - Contém a versão do banco de dados de assinatura de vírus, data, local rastreado, número de objetos rastreados, número de ameaças encontradas, número de regras cumpridas e hora da conclusão.
- **Proteção do servidor de correio -** Todas as mensagens classificadas pelo ESET Mail Security como spam ou provável spam são registradas aqui. Esses relatórios são aplicáveis aos tipos de proteção a seguir: Antispam, Regras e Antivírus.
- **Lista cinza** - Todas as mensagens que forem classificadas usando o método de lista cinza são registradas aqui.

Em cada seção, as informações exibidas podem ser copiadas para a área de transferência (atalho do teclado: Ctrl + C), selecionando a entrada e clicando em **Copiar**. Para selecionar várias entradas, as teclas CTRL e SHIFT podem ser usadas.

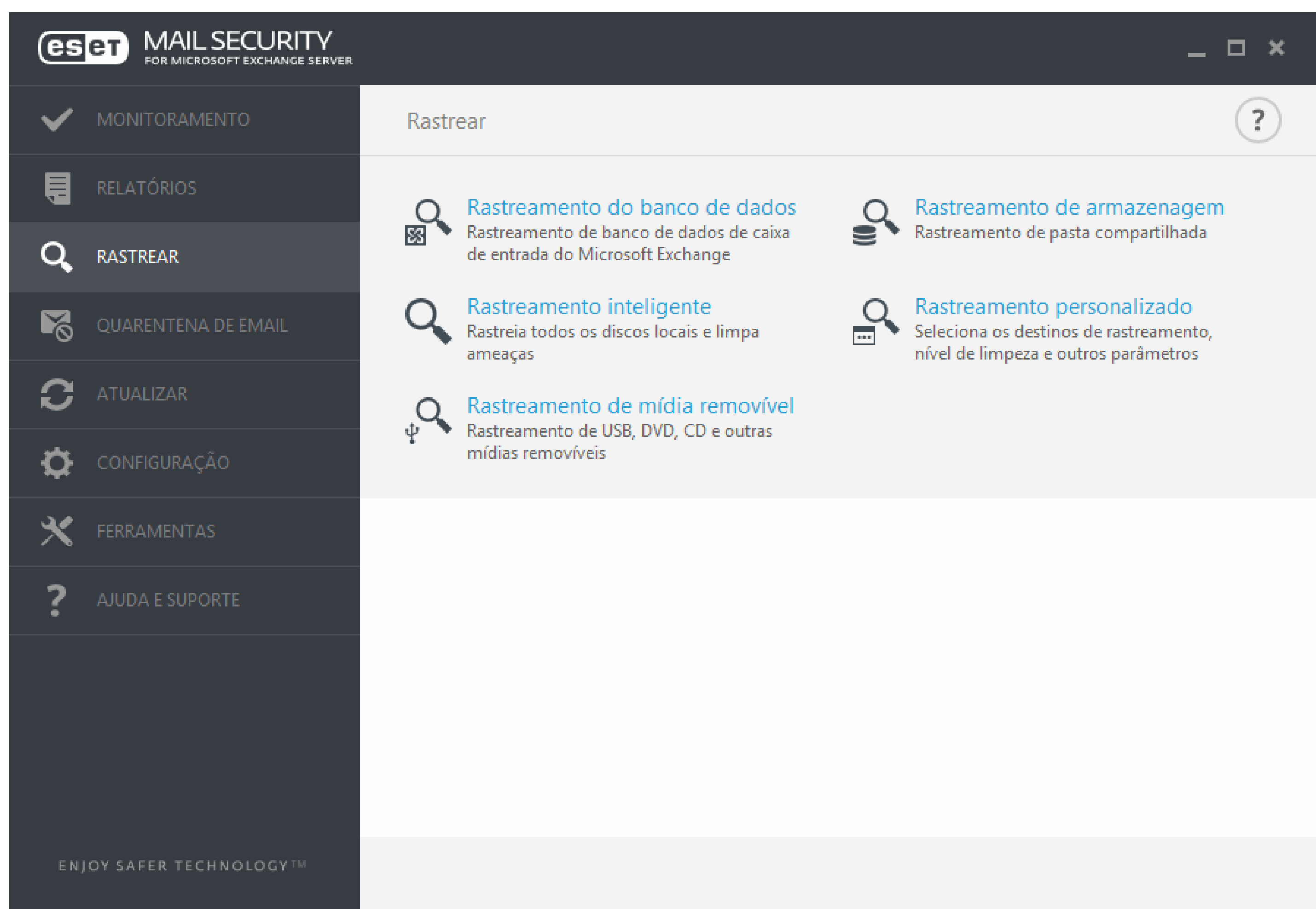
Clique no ícone **Filtragem** para abrir a janela **Filtragem de relatórios** onde poderá definir os critérios de filtragem.

Você pode exibir o menu de contexto clicando com o botão direito em um registro específico. As seguintes opções também estão disponíveis no menu de contexto:

- **Mostrar** - Mostra informações mais detalhadas sobre o relatório selecionado em uma nova janela (igual a um clique duplo).
- **Filtrar os mesmos registros** - Ativa a filtragem de relatório, e exibir apenas relatórios do mesmo tipo que o selecionado.
- **Filtrar...** - Depois de clicar nessa opção, a janela Filtragem de relatórios permitirá que você defina critérios de filtragem para entradas de relatório específicas.
- **Ativar filtro** - Ativa configurações de filtro. Na primeira vez que você filtrar relatórios, será preciso definir seus critérios de filtragem. Assim que os filtros forem definidos, eles continuarão inalterados até que sejam editados.
- **Copiar** - Copia informações dos registros selecionados/destacados para a área de transferência.
- **Copiar tudo** - Copia informações de todos os registros na janela.
- **Excluir** - Exclui os registros selecionados/destacados - esta ação requer privilégios de administrador.
- **Excluir tudo** - Exclui todos os registros na janela - esta ação requer privilégios de administrador.
- **Exportar...** - Exporta informações dos registros selecionados/destacados para um arquivo XML.
- **Exportar todos...** - Exporta todas as informações na janela em um arquivo XML.
- **Localizar...**- Abre uma janela Localizar no relatório e permite que você defina os critérios de busca. Trabalha em conteúdos que já foram filtrados, como uma forma adicional de refinar resultados.
- **Localizar próximo** - Localiza a próxima ocorrência de uma pesquisa definida anteriormente (acima).
- **Localizar anterior** - Localiza a ocorrência anterior de uma pesquisa definida anteriormente (acima).
- **Percorrer relatório** - Deixe esta opção ativada para percorrer automaticamente relatórios antigos e monitorar relatórios ativos na janela **Relatórios**.

4.3 Rastrear

O rastreador sob demanda é uma parte importante do ESET Mail Security. Ele é usado para realizar rastreamentos nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. Recomendamos que você realize rastreamentos detalhados regulares do sistema (por exemplo, uma vez por mês) para detectar vírus que não tenham sido capturados pela Proteção em tempo real do sistema de arquivos. Isso pode acontecer se a Proteção em tempo real do sistema de arquivos estiver desativada no momento, se o banco de dados de vírus for obsoleto ou se o arquivo não for detectado como vírus ao ser salvo no disco.



Há dois tipos de **Rastreamento do computador** disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

Leia Progresso do rastreamento para obter mais informações sobre o processo de rastreamento.

Rastreamento de armazenagem

Rastrear todas as pastas compartilhadas no servidor local. Caso o **Rastreamento de armazenagem** não esteja disponível, isso significa que não há pastas compartilhadas no seu servidor.

Rastreamento Hyper-V

Esta opção é visível no menu apenas se o Gerenciados Hyper-V estiver instalado no servidor que executa o ESET Mail Security. O rastreamento Hyper-V permite rastrear discos de Máquina Virtual (VM) no Servidor Microsoft Hyper-V sem precisar de nenhum “Agente” instalado na VM em particular. Consulte Rastreamento Hyper-V para mais informações.

Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem do Rastreamento inteligente é que ele é fácil de operar e não requer configuração de rastreamento detalhada. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza.

Rastreamento personalizado

O rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de rastreamento, selecione **Rastreamento do computador** > **Rastreamento personalizado** e selecione uma opção no menu suspenso **Alvos de rastreamento** ou selecione alvos específicos na estrutura em árvore. Um alvo de rastreamento pode ser também especificado por meio da inserção do caminho da pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione **Rastrear sem limpar**. Ao realizar um rastreamento, você pode selecionar entre três níveis de limpeza clicando em **Configuração** > **Parâmetros ThreatSense** > **Limpeza**.

A realização de rastreamentos de computador com o Rastreamento personalizado só é recomendada para usuários avançados com experiência anterior na utilização de programas antivírus.

Rastreamento de mídia removível

Semelhante ao rastreamento inteligente - inicie rapidamente um rastreamento de mídia removível (como CD/DVD/USB) conectada ao computador. Isso pode ser útil quando você conectar uma unidade flash USB a um computador e quiser rastrear seu conteúdo quanto a malware e ameaças em potencial.

Esse tipo de rastreamento também pode ser iniciado clicando em **Rastreamento personalizado** e selecionando **Mídia removível** no menu suspenso **Alvos de rastreamento** e clicando em **Rastrear**.

Repetir o último rastreamento

Executa o último rastreamento, qualquer que ele seja (Armazenagem, Inteligente, Personalizado, etc.), com as mesmas configurações.

i **OBSERVAÇÃO:** Recomendamos que execute um rastreamento do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

4.3.1 Rastreamento Hyper-V

O rastreamento antivírus Hyper-V oferece a capacidade de rastrear os discos de um Servidor Microsoft Hyper-V, ou seja, uma Máquina Virtual (VM), sem precisar ter nenhum Agente instalado naquela VM em particular. O antivírus é instalado usando os privilégios do Administrador do servidor Hyper-V.

O rastreamento Hyper-V é derivado do módulo de rastreamento do computador sob demanda, enquanto alguns recursos não foram implementados (rastreamento do Setor de inicialização - será implementado mais tarde, rastreamento da Memória operacional).

Sistemas operacionais compatíveis

- Windows Server 2008 R2 - Máquinas Virtuais executando este sistema operacional podem ser rastreadas apenas se estiverem off-line
- Windows Server 2012
- Windows Server 2012 R2

Requisitos de hardware

O servidor não deve ter nenhum problema de desempenho executando as Máquinas Virtuais. O próprio rastreamento em sua maioria usa apenas os recursos de CPU.
No caso de rastreamento online o espaço em disco livre da VM é necessário. O espaço em disco livre (disponível para uso) deve ser no mínimo o dobro do espaço usado pelos instantâneos e discos virtuais.

A Máquina Virtual a ser rastreada está off-line (desligada)

Com ajuda do Gerenciamento Hyper-V e suporte dos discos virtuais, nós detectamos os discos do sistema operacional na Máquina Virtual e conectamos a eles. Assim temos o mesmo acesso ao conteúdo dos discos que teríamos se estivéssemos acessando arquivos de um disco rígido geral.

Máquina Virtual a ser rastreada (em execução, pausada, salva)

Com ajuda do Gerenciamento Hyper-V e suporte dos discos virtuais, nós detectamos os discos do sistema operacional na Máquina Virtual. A conexão genérica aos discos não está disponível no momento, portanto criamos um instantâneo da Máquina Virtual e, através do instantâneo, conectamos os discos no modo somente leitura. Depois da conclusão do rastreamento, o instantâneo é excluído.
A criação de um instantâneo é uma operação lenta e pode levar de alguns segundos até um minuto. Isso deve ser considerado ao aplicar o rastreamento Hyper-V em quantidades maiores de Máquinas Virtuais.

OBSERVAÇÃO: Até agora o rastreamento Hyper-V é apenas um rastreamento somente leitura para as Máquinas Virtuais on-line e off-line. A capacidade de limpar infiltrações detectadas será implementada em um momento posterior.

Convenção de nomeação

O módulo do rastreamento Hyper-V usa a seguinte convenção de nomeação:
`NomeMáquinaVirtual\DiscoX\VolumeY`

onde X é o número do disco e Y é o número do volume.
Por exemplo: "`Computador\Disco0\Volume1`".

O sufixo de número é adicionado com base na ordem de detecção, que é idêntica à ordem vista no Gerenciador de Discos da VM.
Essa convenção de nomeação é usada na lista estruturada em árvore de destinos a serem rastreados, na barra de progresso e também nos relatórios.

Executando um rastreamento

Um rastreamento pode ser executado de 3 formas:

- Sob demanda - Se você clicar na opção de rastreamento Hyper-V no menu do ESET Mail Security, você verá uma lista de Máquinas Virtuais (se existirem) disponíveis para serem rastreadas. É uma lista em estrutura de árvore onde a entidade de menor nível a ser rastreada é um volume, o que significa que não é possível escolher um diretório ou arquivo a ser rastreado, pelo menos o volume completo deve ser rastreado.
  Para listar os volumes disponíveis, temos que conectar ao(s) disco(s) virtual(is) em particular e isso pode levar alguns segundos. Portanto, uma opção mais rápida é marcar uma Máquina Virtual ou seu(s) disco(s) a ser(em) rastreado(s).
  Assim que tiver marcado as Máquinas Virtuais, discos ou volumes a serem rastreados, clique no botão Rastrear.
- Através da agenda
- Através do ERA como uma Tarefa de cliente chamada de Rastrear servidor. O menor nível a ser rastreado é um disco de uma Máquina Virtual.

É possível executar vários rastreamentos Hyper-V simultaneamente.

Assim que o rastreamento for concluído, você verá uma notificação e um link Exibir relatório através do qual será possível revisar os detalhes do rastreamento executado. Todos os relatórios de rastreamento estão disponíveis na seção Relatórios de rastreamento do ESET Mail Security, mas é preciso escolher Rastreamento Hyper-V no menu suspenso para ver os relatórios relacionados.

Possíveis problemas

- Ao executar o rastreamento de uma Máquina Virtual on-line, um instantâneo da Máquina Virtual em particular deve ser criado e, durante a criação de um instantâneo, algumas ações genéricas da Máquina Virtual podem ser limitadas ou desativadas.
- Se uma Máquina Virtual estiver sendo rastreada, ela não pode ser ligada até que o rastreamento seja concluído.
- O Gerenciador Hyper-V Manager permite nomear duas Máquinas Virtuais diferentes de forma idêntica, e isso é um problema ao tentar diferenciar as máquinas ao revisar os relatórios de rastreamento.

4.4 Quarentena de email

O gerente de quarentena de email está disponível para todos os três tipos de quarentena:

- Quarentena local
- Quarentena da caixa de entrada
- Quarentena do MS Exchange

OBSERVAÇÃO: A Interface web de quarentena de email é uma alternativa ao gerente de quarentena de email, que permite gerenciar os objetos de quarentena de email.

Filtragem

- **Período de tempo** - você pode selecionar um Período de tempo durante o qual os emails são exibidos (o padrão é uma semana). Quando alterar o Período de tempo, os itens da Quarentena de email são recarregados automaticamente.
- **Filtro** - você pode usar a caixa de texto de filtro para filtrar emails exibidos (todas as colunas são pesquisadas).

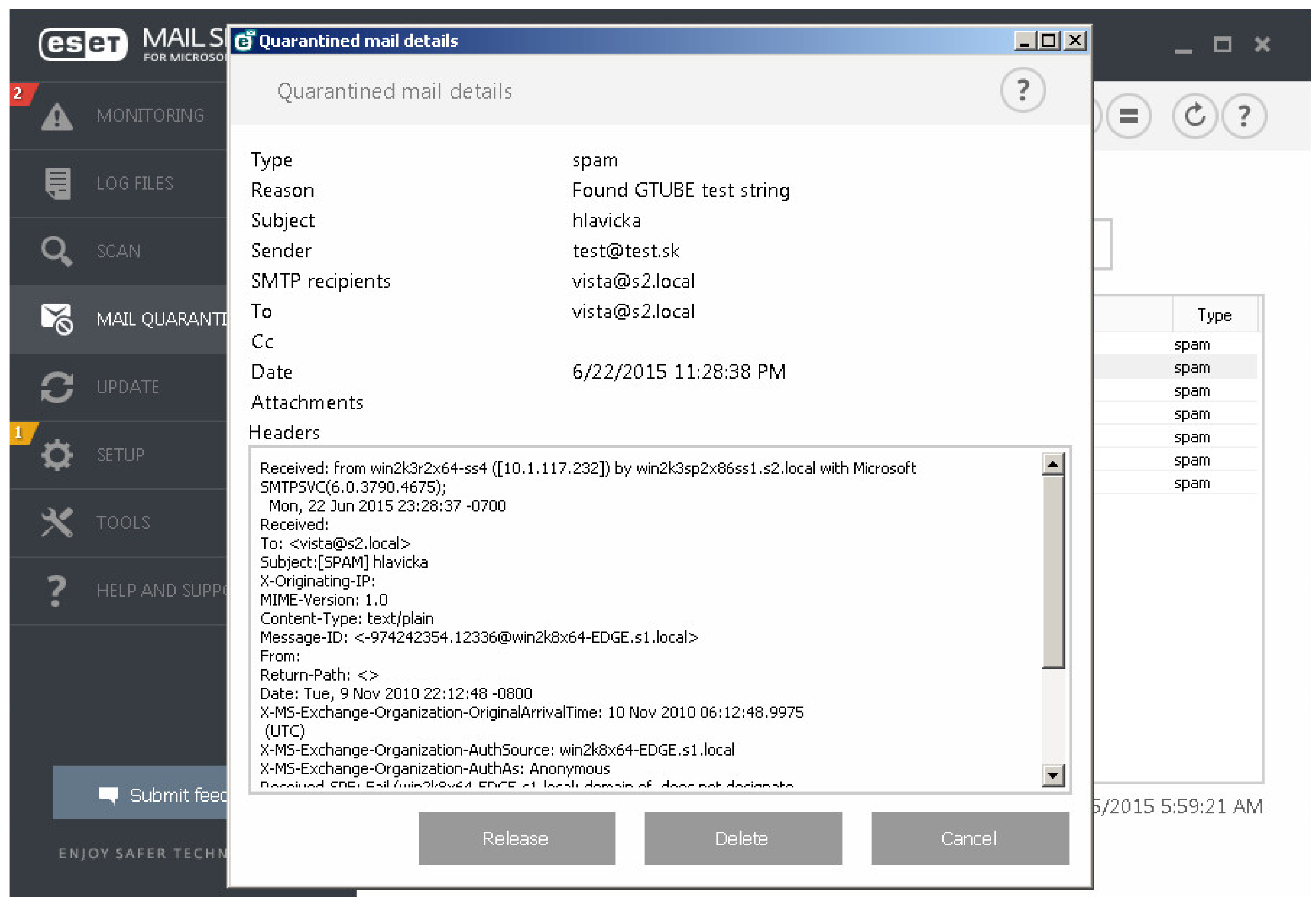
OBSERVAÇÃO: Dados do gerente de quarentena de email não são atualizados automaticamente, recomendamos clicar em atualizar regularmente para ver os itens mais atuais na Quarentena de email.

Ação

- **Lançamento** - lança o email ao seu destinatário original usando o diretório de reprodução, e exclui o email da quarentena. Clique em **Sim** para confirmar a ação.
- **Excluir** - exclui itens da quarentena. Clique em **Sim** para confirmar a ação.

Detalhes do email na quarentena - clique duas vezes na mensagem em quarentena ou clique com o botão direito e selecione **Detalhes** e uma janela pop-up vai abrir com os detalhes sobre o email em quarentena. Você também pode encontrar algumas informações adicionais sobre o email no cabeçalho de email RFC.

Ações também estão disponíveis no menu de contexto. Se quiser, clique em **Lançamento**, **Excluir** ou **Excluir permanentemente** para realizar uma ação com uma mensagem de email em quarentena. Clique em **Sim** para confirmar a ação. Se escolher **Excluir permanentemente** a mensagem também será excluída do sistema de arquivos, ao contrário de **Excluir** que vai remover o item da item exibição do Gerente de quarentena de email.



4.4.1 Detalhes do email em quarentena

Esta janela contém informações sobre a mensagem de email em quarentena como **Tipo**, **Motivo**, **Assunto**, **Remetente**, **Destinatários SMTP**, **Para**, **CC**, **Data**, **Anexos** e **Cabeçalhos**. Você pode selecionar, copiar e colar os cabeçalhos se precisar.

Você pode realizar uma ação com a mensagem de email em quarentena usando os botões:

- **Lançamento** - lança o email ao seu destinatário original usando o diretório de reprodução, e exclui o email da quarentena. Clique em **Sim** para confirmar a ação.
- **Excluir** - exclui itens da quarentena. Clique em **Sim** para confirmar a ação.

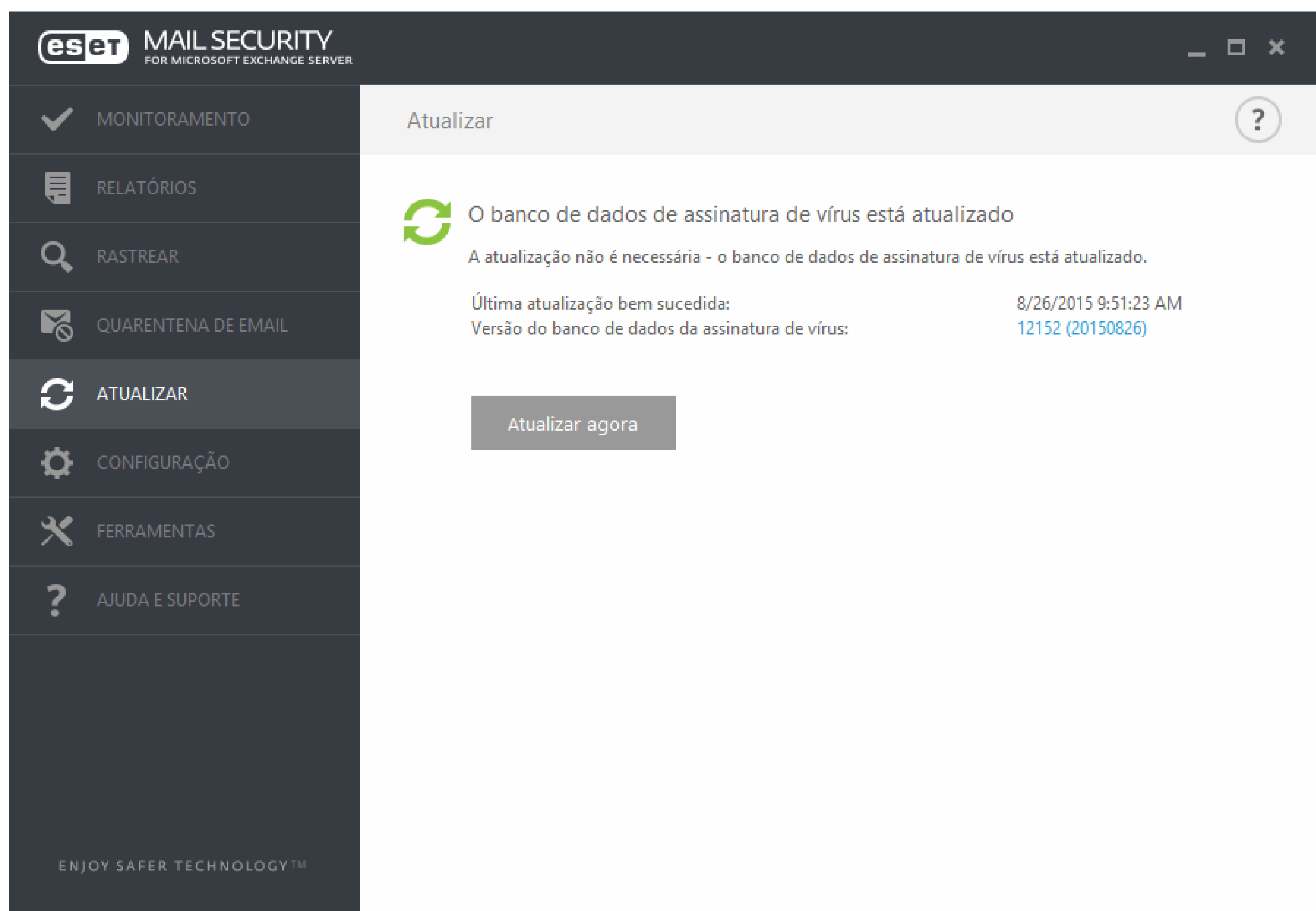
Clicar no botão **Cancelar** vai fechar a janela de detalhes de email em quarentena.

4.5 Atualizar

Atualizar o ESET Mail Security periodicamente é o melhor método para se manter o nível máximo de segurança em seu computador. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras, atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

Na janela principal do programa, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

Para começar o processo de atualização, clique em **Atualizar agora**. A atualização do banco de dados de assinatura de vírus e a atualização dos componentes do programa são partes importantes da manutenção da proteção completa contra códigos maliciosos.



Última atualização bem-sucedida - A data da última atualização. Verifique se ela se refere a uma data recente, o que significa que o banco de dados de assinatura de vírus está atualizado.

Versão do banco de dados de assinatura de vírus – O número do banco de dados de assinatura de vírus, que também é um link ativo para o site da ESET. Clique para exibir uma lista de todas as assinaturas adicionadas em uma determinada atualização.

Processo de atualização

Depois de clicar em **Atualizar agora**, o processo de download começa e o progresso da atualização será exibido. Para interromper a atualização, clique em **Cancelar atualização**.

Importante: Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem **A atualização não é necessária - O banco de dados de assinatura de vírus está atualizado** aparecerá na janela **Atualizar**. Se esse não for o caso, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize o banco de dados de assinatura de vírus assim que for possível. Caso contrário, uma das seguintes mensagens será exibida:

O banco de dados de assinatura de vírus está desatualizado - Esse erro aparecerá após diversas tentativas malsucedidas de atualizar o banco de dados de assinatura de vírus. Recomendamos que você verifique as configurações de atualização. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos ou definições incorretas das configurações de conexão.

A notificação anterior está relacionada às duas mensagens a seguir de **Falha na atualização do banco de dados de assinatura de vírus** sobre atualizações malsucedidas:

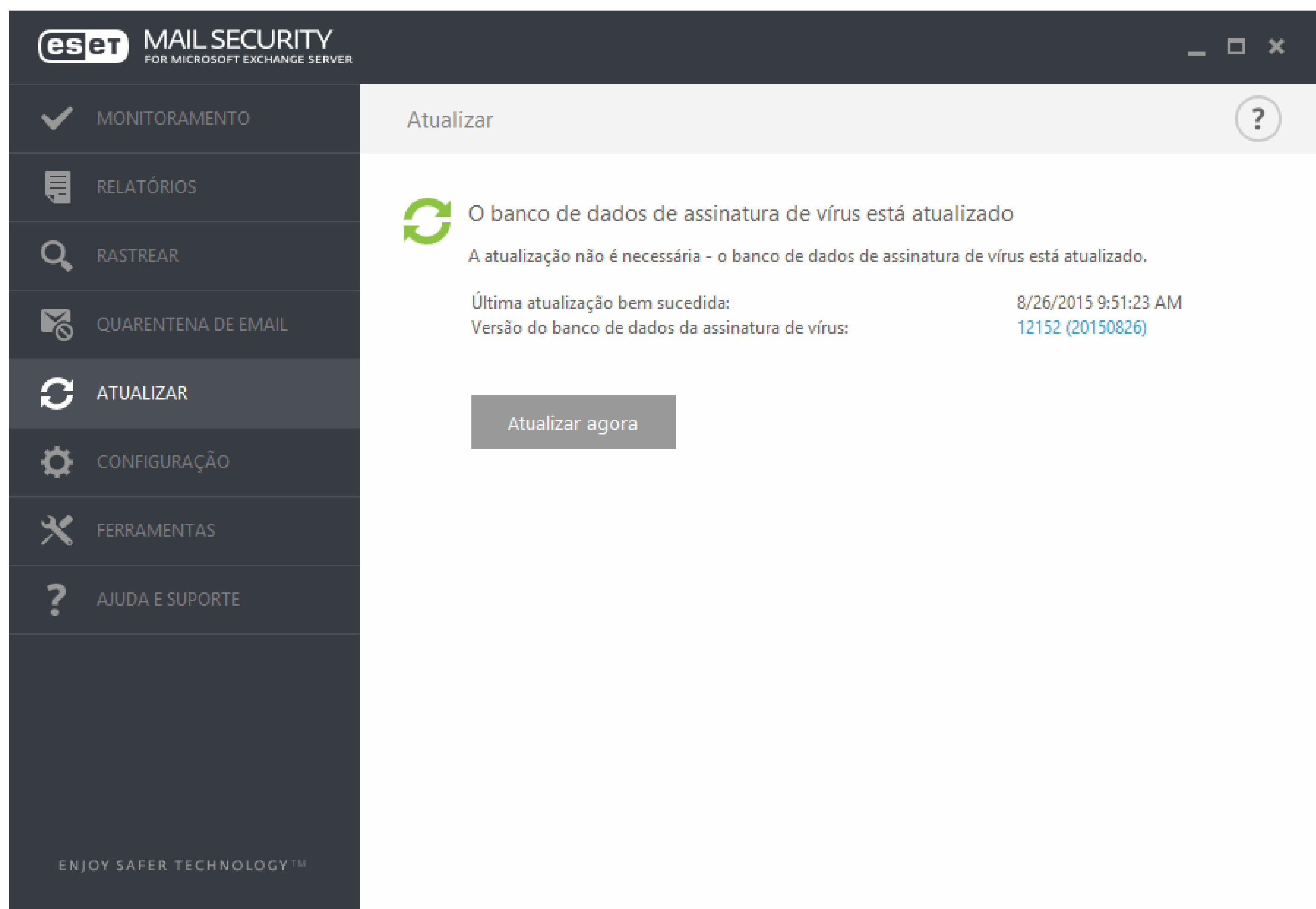
Licença inválida - A chave de licença foi inserida incorretamente na configuração da atualização. Recomendamos que você verifique os seus dados de autenticação. A janela Configuração avançada (pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Ajuda e suporte** > **Gerenciar licenças** a partir do menu principal para inserir uma nova chave de licença.

Ocorreu um erro durante o download dos arquivos de atualização - Uma possível causa desse erro pode dever-se a configurações de conexão à Internet incorretas. Recomendamos que você verifique a conectividade da Internet abrindo qualquer site em seu navegador da Web. Se o site não abrir, é provável que uma conexão com a Internet não tenha sido estabelecida ou que haja problemas de conectividade com o seu computador. Verifique com o seu provedor de serviços de Internet (ISP) se você não tiver uma conexão ativa com a Internet.

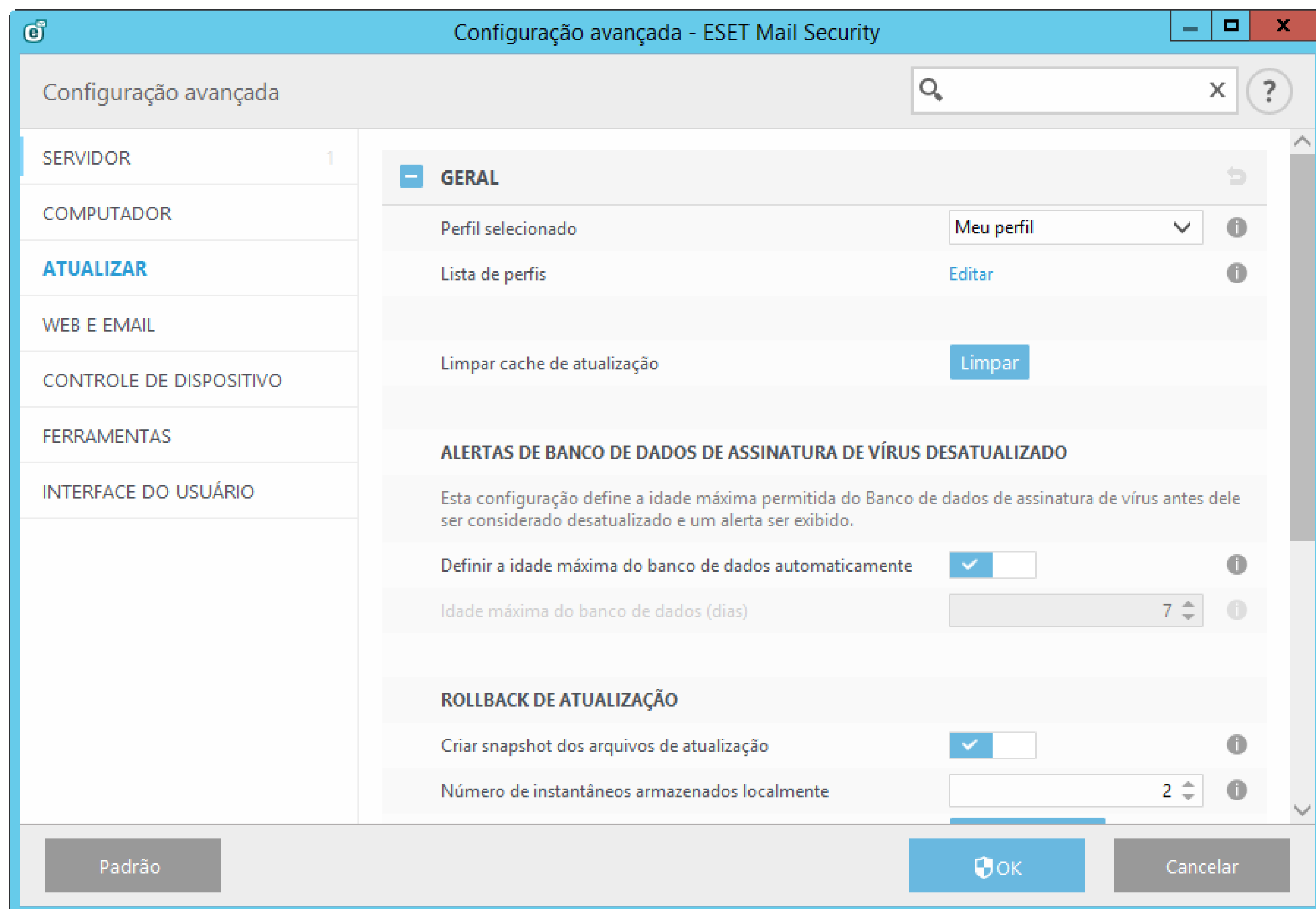
i **OBSERVAÇÃO:** Para obter mais informações, acesse este artigo da Base de conhecimento ESET.

4.5.1 Estabelecendo atualização de banco de dados de vírus

A atualização do banco de dados de assinatura de vírus e dos componentes do programa é uma parte importante no fornecimento de proteção completa contra códigos maliciosos. Preste bastante atenção à sua configuração e operação. No menu principal, vá para **Atualizar** e clique em **Atualizar agora** para verificar se há um banco de dados de assinatura mais recente.



Você pode definir as configurações de atualização na janela de Configuração avançada (pressione a tecla F5 no seu teclado). Para configurar as opções avançadas de atualização, como o modo de atualização, o acesso ao servidor proxy, a conexão de rede e as configurações de criação de cópias do banco de dados de assinatura de vírus (imagem), clique em **Atualizar** na janela de **Configuração avançada** à esquerda. Se tiver problemas com uma atualização, clique em **Limpar cache** para limpar a pasta com arquivos de atualização temporários. Por padrão, o menu **Servidor de atualização** está definido como **SELEÇÃO AUTOMÁTICA**. **SELEÇÃO AUTOMÁTICA** significa que o servidor de atualização, do qual as atualizações de assinatura de vírus foram baixadas, é selecionado automaticamente. Recomendamos que você deixe a opção padrão selecionada. Se você não quiser que a notificação da bandeja do sistema no canto inferior direito da tela seja exibida, selecione **Desativar exibir notificação sobre atualização bem-sucedida**.

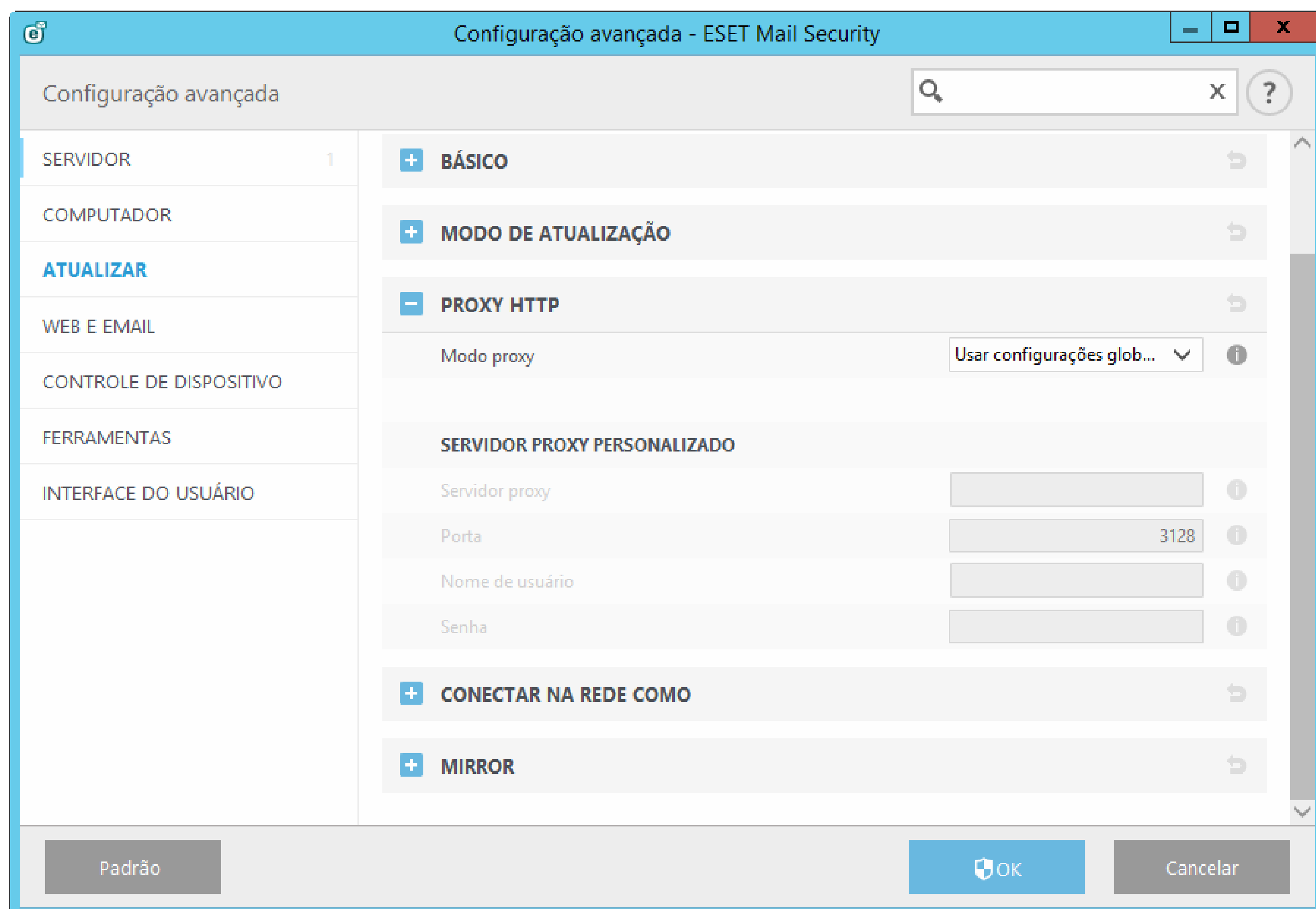


Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Essa ação somente será possível se a **Chave de licença** correta for inserida em **Ajuda e suporte** > **Ativar licença**.

Se você não ativou seu produto após a instalação, poderá ativá-lo a qualquer momento. Para obter informações mais detalhadas sobre a ativação, consulte Como ativar o ESET Mail Security e insira os dados de licença recebidos com o produto de segurança ESET na janela Detalhes da licença.

4.5.2 Configuração do servidor proxy para atualizações

Se estiver usando um servidor proxy para a conexão à Internet em um sistema onde o ESET Mail Security está instalado, as configurações de proxy devem estar configuradas em Configuração avançada. Para acessar a janela de configuração do servidor proxy, pressione F5 para abrir a janela Configuração avançada e clique em **Atualizar** > **Proxy HTTP**. Selecione **Conexão através de um servidor proxy** no menu suspenso **Modo proxy** e preencha os detalhes do seu servidor proxy: **Servidor proxy** (endereço IP), número da **Porta** e **Nome de usuário** e **Senha** (se aplicável).



Se você não estiver certo sobre os detalhes do servidor proxy, pode tentar detectar automaticamente suas configurações do servidor proxy ao selecionar **Usar configurações globais de servidor proxy** na lista suspensa.

OBSERVAÇÃO: As opções de servidor proxy para diferentes perfis de atualização podem variar. Se for este o caso, configure os diferentes perfis de atualização na Configuração avançada, clicando em **Atualizar** > **Perfil**.

4.6 Configurar

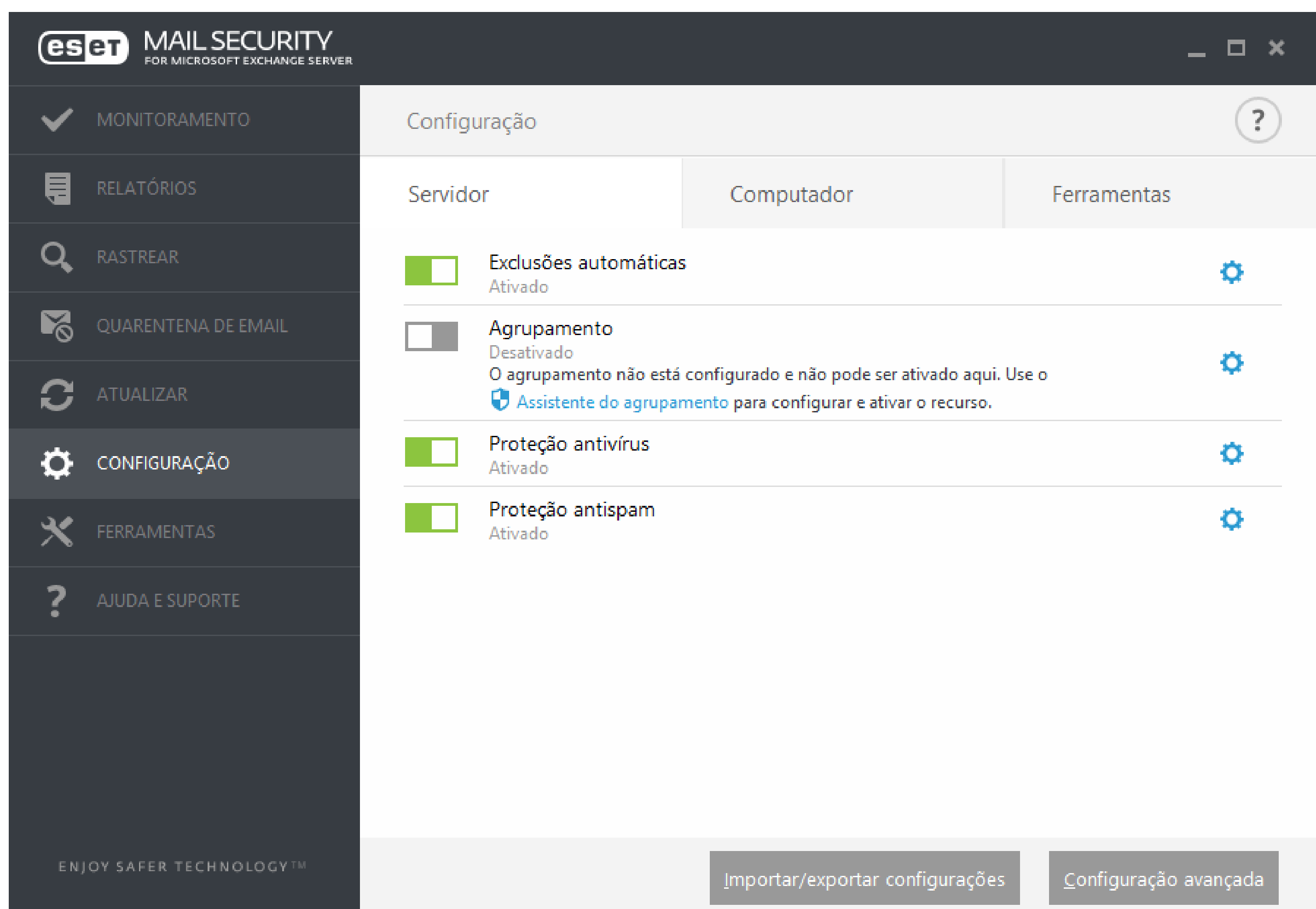
O menu de configuração é composto por em três guias:

- Servidor
- Computador
- Ferramentas

4.6.1 Servidor

O ESET Mail Security oferece proteção para seu servidor com recursos essenciais, como: Antivírus e Antispyware, Proteção residente (Proteção em tempo real), proteção do acesso à Web e Proteção do cliente de email. Você pode ler mais sobre cada tipo de proteção em ESET Mail Security - Proteção do computador.

- Exclusões automáticas este recurso identifica aplicativos críticos de servidor e arquivos do sistema operacional do servidor e os adiciona automaticamente à lista de Exclusões. Essa funcionalidade reduzirá o risco de possíveis conflitos e aumenta o desempenho geral do servidor ao executar o software antivírus.
- Para configurar o Agrupamento ESET, clique em **Assistente do agrupamento.** Para obter detalhes sobre como configurar o Agrupamento ESET usando o assistente, clique aqui.



Se quiser definir opções com mais detalhes, clique em **Configuração avançada** ou pressione **F5**.

Existem opções adicionais na parte inferior da janela de configuração. Para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar os parâmetros atuais em um arquivo de configuração, use a opção **Importar e exportar configurações**. Para obter informações mais detalhadas, consulte Importar/Exportar configurações.

4.6.2 Computador

o ESET Mail Security tem todos os componentes necessários para garantir proteção suficiente do servidor como um computador. Cada componente oferece um tipo específico de proteção, como: Antivírus e antispyware, Proteção em tempo real do sistema de arquivos, Acesso a web, Cliente de email, Proteção antiphishing, etc.

A seção **Computador** pode ser encontrada em **Configuração** > **Computador**. Você verá uma lista de componentes que você pode ativar/desativar usando a chave . Para definir as configurações de um item específico, clique na engrenagem . Para **Proteção em tempo real do sistema de arquivos**, também há a opção de **Editar exclusões**, que abrirá a janela de configuração de Exclusões onde você pode excluir arquivos e pastas do rastreamento.

Pausar a Proteção antivírus e antispyware - A qualquer momento que você desativar temporariamente a Proteção antivírus e antispyware, você poderá selecionar o período de tempo para o qual deseja que o componente selecionado seja desativado usando o menu suspenso e então clicar em **Aplicar** para desativar o componente de segurança. Para reativar a proteção, clique em **Ativar proteção antivírus e antispyware**.

O módulo do **Computador** permite que você ative/desative e configure os componentes a seguir:

- **Proteção em tempo real do sistema de arquivos** – Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador.
- **Proteção de documentos** - O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, como, por exemplo, elementos do Microsoft ActiveX.
- **Controle de dispositivo** - Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo.
- **HIPS** - O sistema HIPS monitora os eventos que ocorrem dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **Modo de apresentação** - Um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela do programa principal será exibida em laranja após a ativação do Modo de apresentação.
- **Proteção Anti-Stealth** - Fornece a detecção de programas nocivos, como os rootkits, que podem se auto-ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.
- **Proteção do acesso à web** - Se ativada, todo o tráfego através de HTTP ou HTTPS será rastreado quanto a software malicioso.
- **Proteção do cliente de email** - Monitora a comunicação recebida através dos protocolos POP3 e IMAP.
- **Proteção antiphishing** - Outra camada de proteção que fornece um nível superior de defesa de sites ilegítimos que tentam adquirir senhas e outras informações confidenciais.

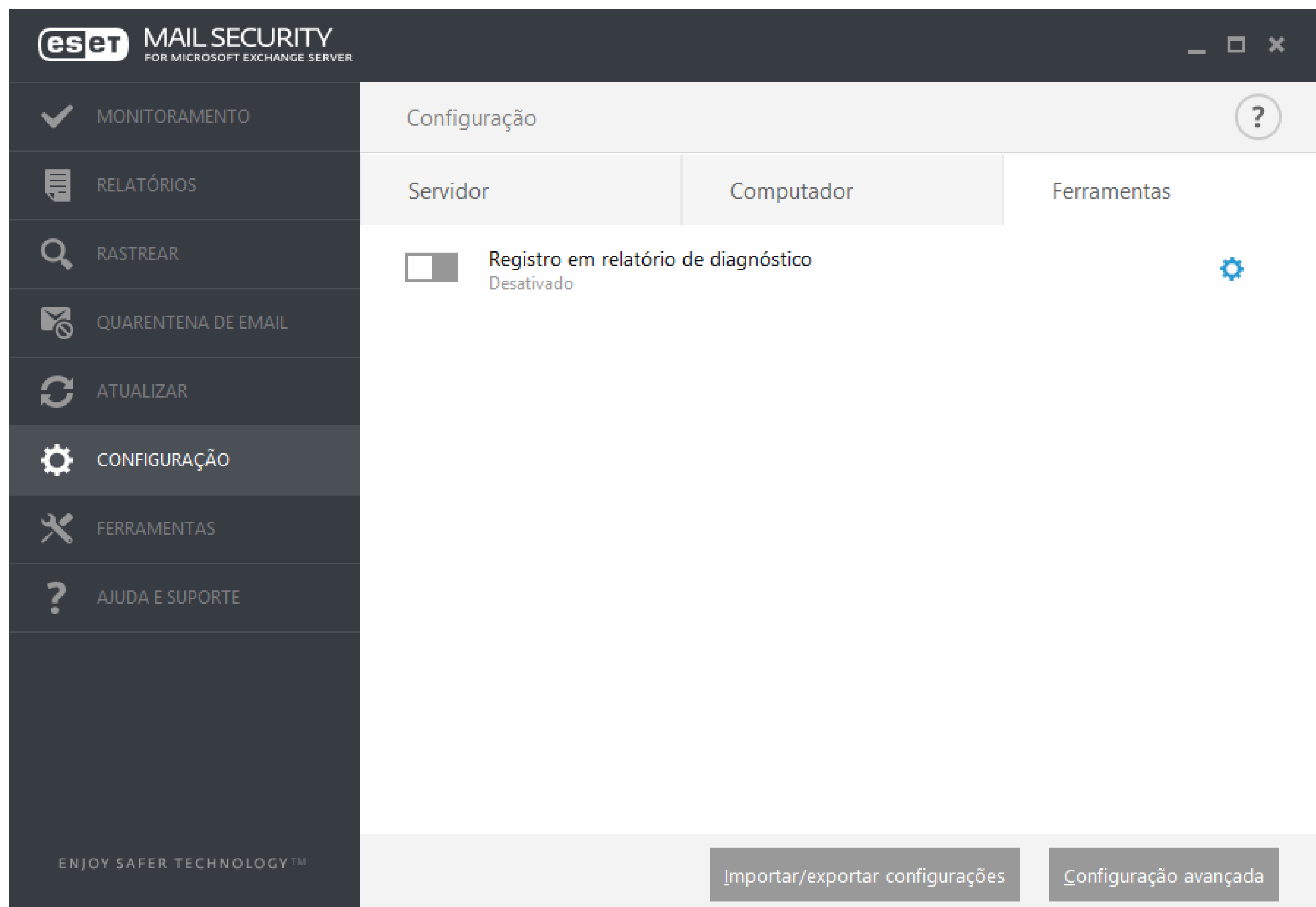
i **OBSERVAÇÃO:** A proteção de documentos está desativada por padrão. Se quiser ela pode ser ativada facilmente clicando do ícone de opção.

Existem opções adicionais na parte inferior da janela de configuração. Para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar os parâmetros atuais em um arquivo de configuração, use a opção **Importar e exportar configurações**. Para obter informações mais detalhadas, consulte Importar/Exportar configurações.

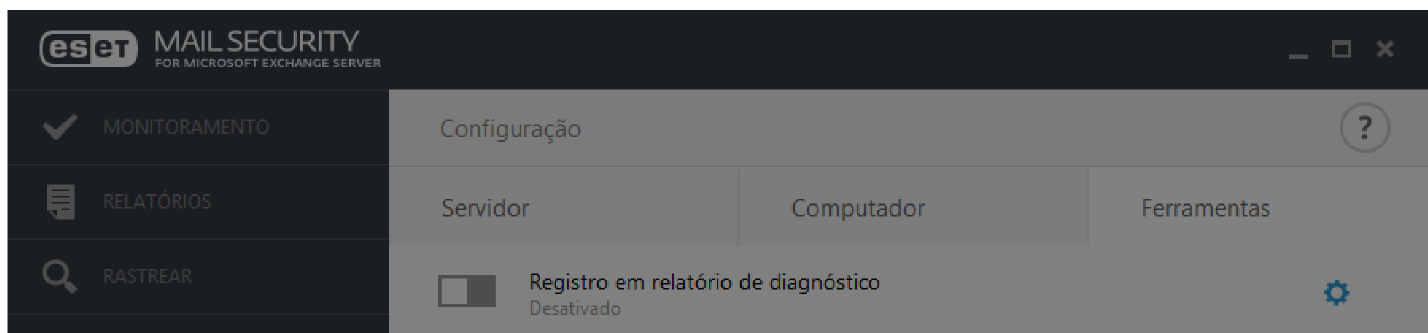
Se quiser definir opções com mais detalhes, clique em **Configuração avançada** ou pressione **F5**.

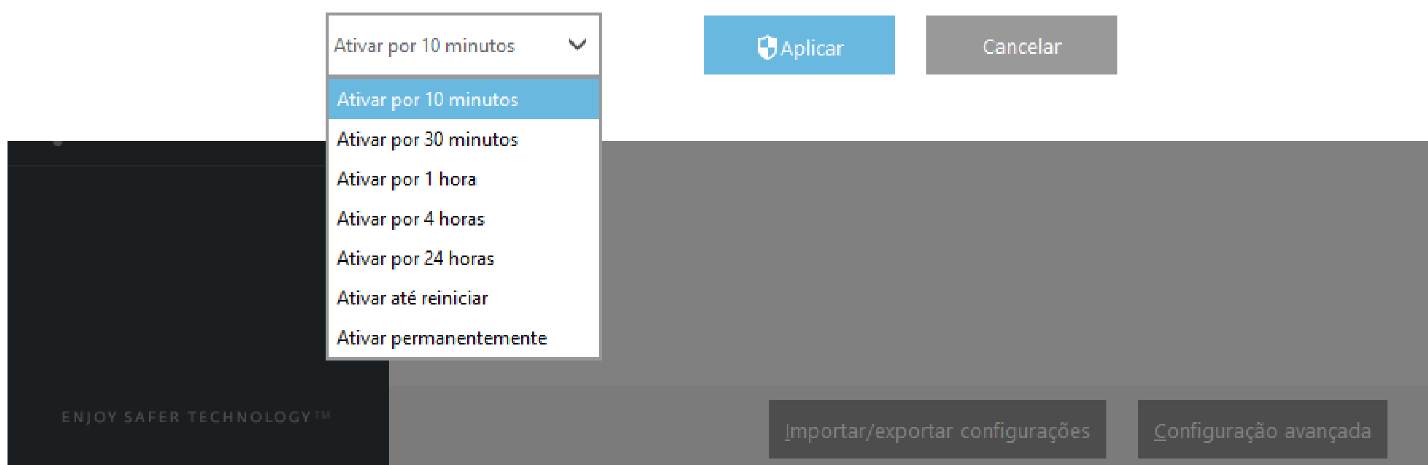
4.6.3 Ferramentas

Registro em relatório de diagnóstico - configura quais componentes vão escrever relatórios de diagnóstico quando o relatório de diagnóstico estiver habilitado. Ao clicar na opção para ativar o registro em relatório de diagnóstico, é possível escolher por quanto tempo ela estará ativada (10 minutos, 30 minutos, 1 hora, 4 horas, 24 horas, até a próxima reinicialização do servidor ou permanentemente). Componentes que não são exibidos nesta guia sempre gravam relatórios de diagnóstico.



- **Ativar** o registro em relatório de diagnóstico para o período de tempo selecionado.

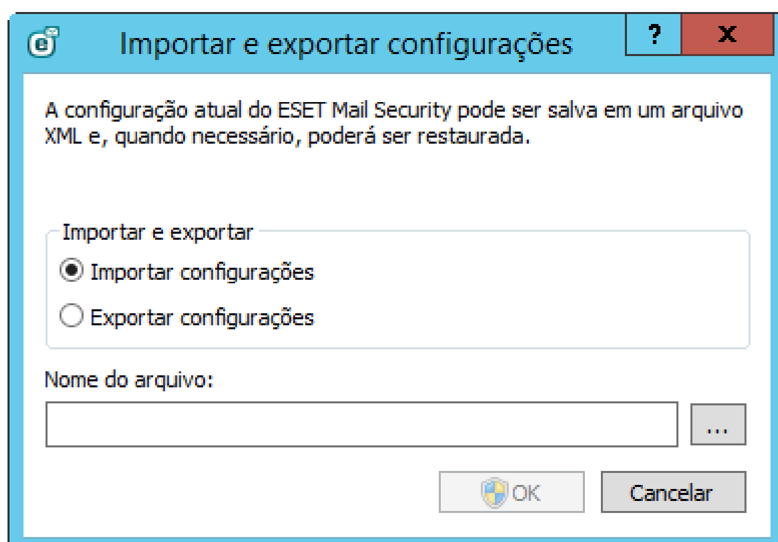




4.6.4 Importar e exportar configurações

Importar e exportar as configurações do ESET Mail Security é possível em **Configuração** clicando em **Importar/ exportar configurações**.

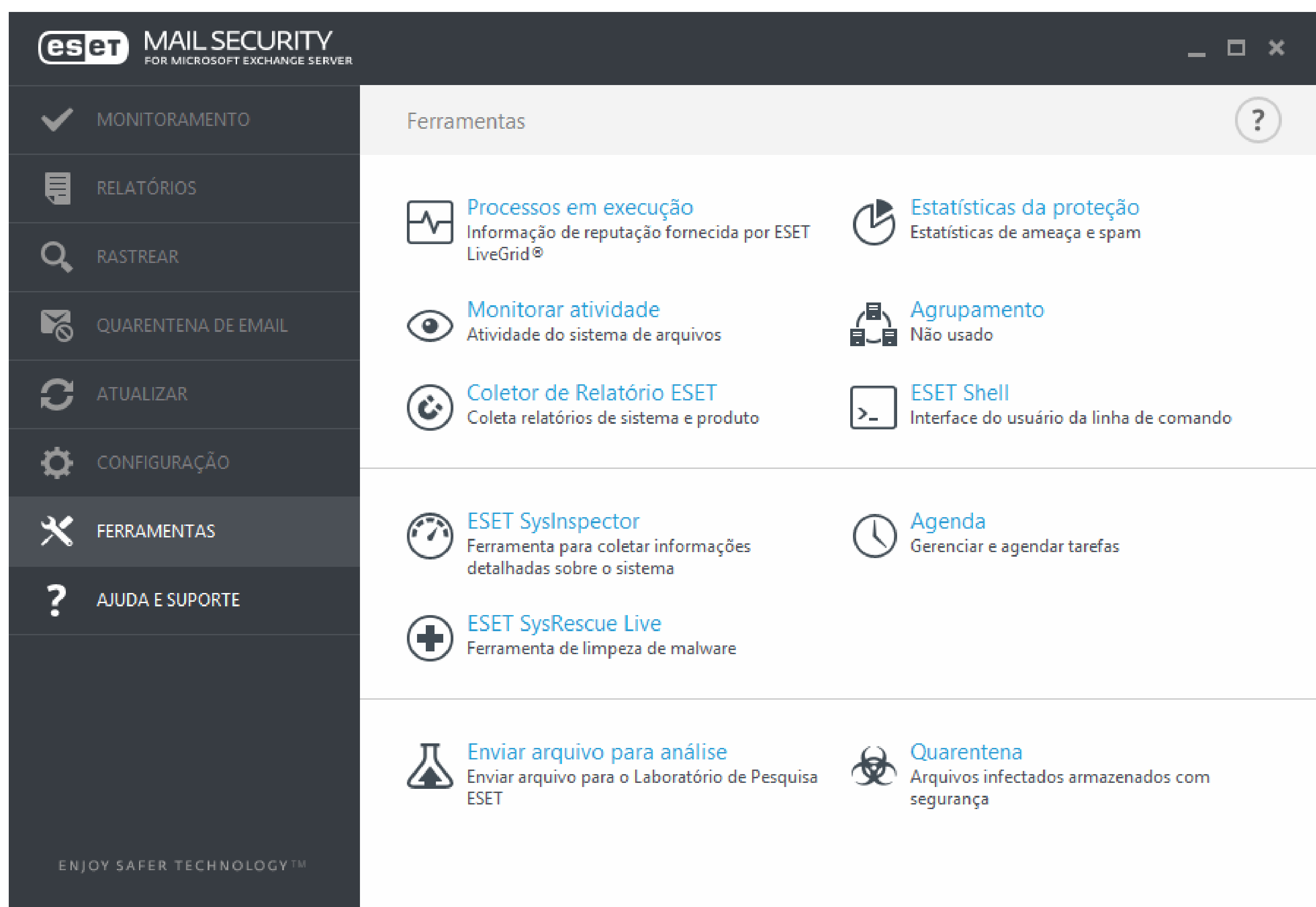
Tanto a importação quanto a exportação utilizam arquivos .xml. A importação e a exportação serão úteis caso precise fazer backup da configuração atual do ESET Mail Security. Pode ser usado posteriormente para aplicar as mesmas configurações a outros computadores.



4.7 Ferramentas

O menu Ferramentas inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais. Ele inclui as seguintes ferramentas:

- Processos em execução
- Monitorar atividade
- ESET Log Collector
- Estatísticas da proteção
- Agrupamento
- ESET Shell
- ESET SysInspector
- ESET SysRescue Live
- Agenda
- Enviar arquivo para análise
- Quarentena



4.7.1 Processos em execução

Os processos em execução exibem os programas ou processos em execução no computador e mantêm a ESET imediatamente e continuamente informada sobre novas infiltrações. O ESET Mail Security oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia ESET Live Grid ativada.

eset MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

MONITORAMENTO
RELATÓRIOS
RASTREAR
QUARENTENA DE EMAIL
ATUALIZAR
CONFIGURAÇÃO
FERRAMENTAS
AJUDA E SUPORTE

ENJOY SAFER TECHNOLOGY™

Processos em execução

Esta janela exibe uma lista de arquivos selecionados com informações adicionais no ESET LiveGrid®. O nível de risco de cada um é indicado, juntamente com o número de usuários e a hora da primeira descoberta.

Ní...	Processo	PID	Número de usu...	Hora da descoberta	Nome do aplicativo
✔	smss.exe	196		um ano atrás	Microsoft® Windows® ...
✔	csrss.exe	296		um ano atrás	Microsoft® Windows® ...
✔	wininit.exe	368		um ano atrás	Microsoft® Windows® ...
✔	winlogon.exe	396		um ano atrás	Microsoft® Windows® ...
✔	services.exe	456		um ano atrás	Microsoft® Windows® ...
✔	lsass.exe	464		um ano atrás	Microsoft® Windows® ...
✔	svchost.exe	596		um ano atrás	Microsoft® Windows® ...
✔	logonui.exe	732		um ano atrás	Microsoft® Windows® ...
✔	dwm.exe	744		um ano atrás	Microsoft® Windows® ...
✔	spoolsv.exe	1200		um ano atrás	Microsoft® Windows® ...
✔	microsoft.activedirecto...	1228		um ano atrás	Microsoft (R) Windows (...
✔	dfsrs.exe	1292		um ano atrás	Microsoft® Windows® ...
✔	dns.exe	1336		um ano atrás	Microsoft® Windows® ...
✔	fms.exe	1380		um ano atrás	Microsoft® Filtering Core

▾ Mostrar detalhes

Nível de risco - Na maioria dos casos, o ESET Mail Security e a tecnologia ESET Live Grid atribui níveis de risco aos objetos (arquivos, processos, chaves de registro etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 – Aceitável (verde) a 9 – Perigoso (vermelho).

Processo - Nome da imagem do programa ou processo em execução no computador. Você também pode usar o Gerenciador de tarefas do Windows para ver todos os processos que estão em execução no computador. O Gerenciador de tarefas pode ser aberto clicando-se com o botão direito em uma área vazia da barra de tarefas e, em seguida, clicando na opção **Ctrl+Shift+Esc** no teclado.

PID - É um ID de processos em execução em sistemas operacionais Windows.

ℹ **OBSERVAÇÃO:** Aplicativos conhecidos marcados como Aceitável (verde) são limpos definitivamente (lista de permissões) e serão excluídos do rastreamento, pois isso melhorará a velocidade do rastreamento sob demanda do computador ou da Proteção em tempo real do sistema de arquivos no computador.

Número de usuários - O número de usuários que utilizam um determinado aplicativo. Estas informações são reunidas pela tecnologia ESET Live Grid.

Hora da descoberta - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia ESET Live Grid.

ℹ **OBSERVAÇÃO:** Quando um aplicativo é marcado com o nível de segurança Desconhecido (laranja), não é necessariamente um software malicioso. Geralmente, é apenas um aplicativo mais recente. Se você não estiver certo em relação ao arquivo, use o recurso Enviar amostra para análise para enviar o arquivo para o Laboratório de

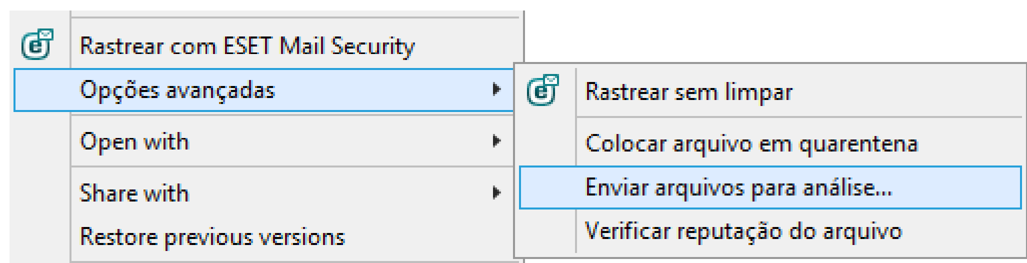
vírus da ESET. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores do banco de dados de assinatura de vírus.

Nome do aplicativo – O nome de um programa ao qual este processo pertence.

Ao clicar em um determinado aplicativo na parte inferior, as seguintes informações serão exibidas na parte inferior da janela:

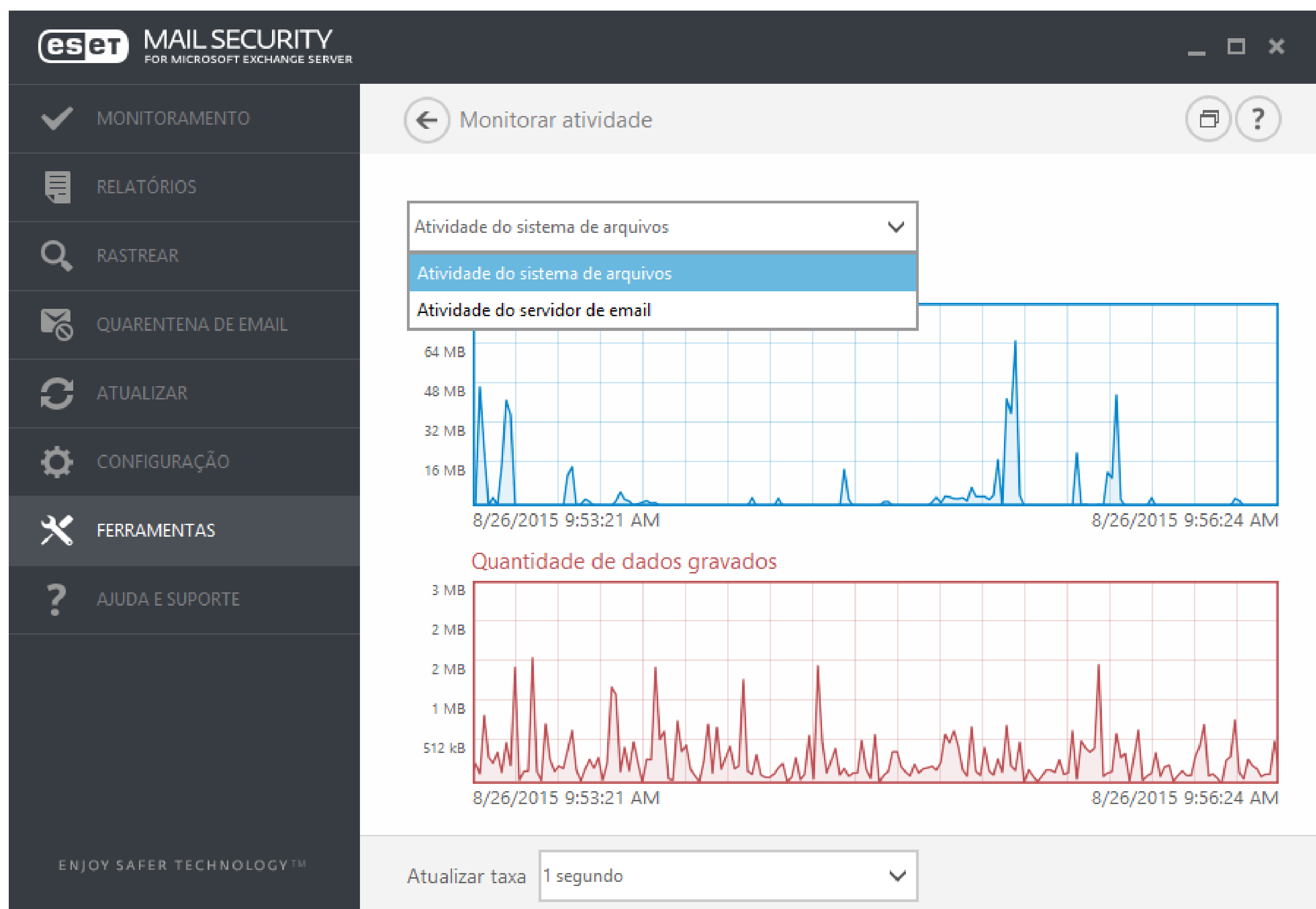
- **Caminho** - Local de um aplicativo no computador.
- **Tamanho** - Tamanho do arquivo em kB (kilobytes) ou MB (megabytes).
- **Descrição** - Características do arquivo com base na descrição do sistema operacional.
- **Companhia** - Nome de processo do aplicativo ou do fornecedor.
- **Versão** - Informações do editor do aplicativo.
- **Produto** - Nome do aplicativo e/ou nome comercial.
- **Criado em** - Data e hora quando um aplicativo foi criado.
- **Modificado em** - Data e hora da última modificação de um aplicativo.

OBSERVAÇÃO: A reputação também pode ser verificada em arquivos que não agem como programas/processos em execução - marque os arquivos que deseja verificar, clique neles com o botão direito do mouse e, no menu de contexto, selecione **Opções avançadas** > **Verificar reputação do arquivo usando o ESET Live Grid**.



4.7.2 Monitorar atividade

Para ver a **Atividade do sistema de arquivos** atual em forma gráfica, clique em **Ferramentas** > **Monitorar atividade**. Mostra a você a quantidade de dados lidos e gravados em seu sistema em dois gráficos. Na parte inferior do gráfico, há uma linha do tempo que grava a atividade do sistema de arquivos em tempo real com base na duração do tempo selecionado. Para alterar a duração do tempo, selecione a partir do menu suspenso **Atualizar taxa**.



As opções disponíveis são:

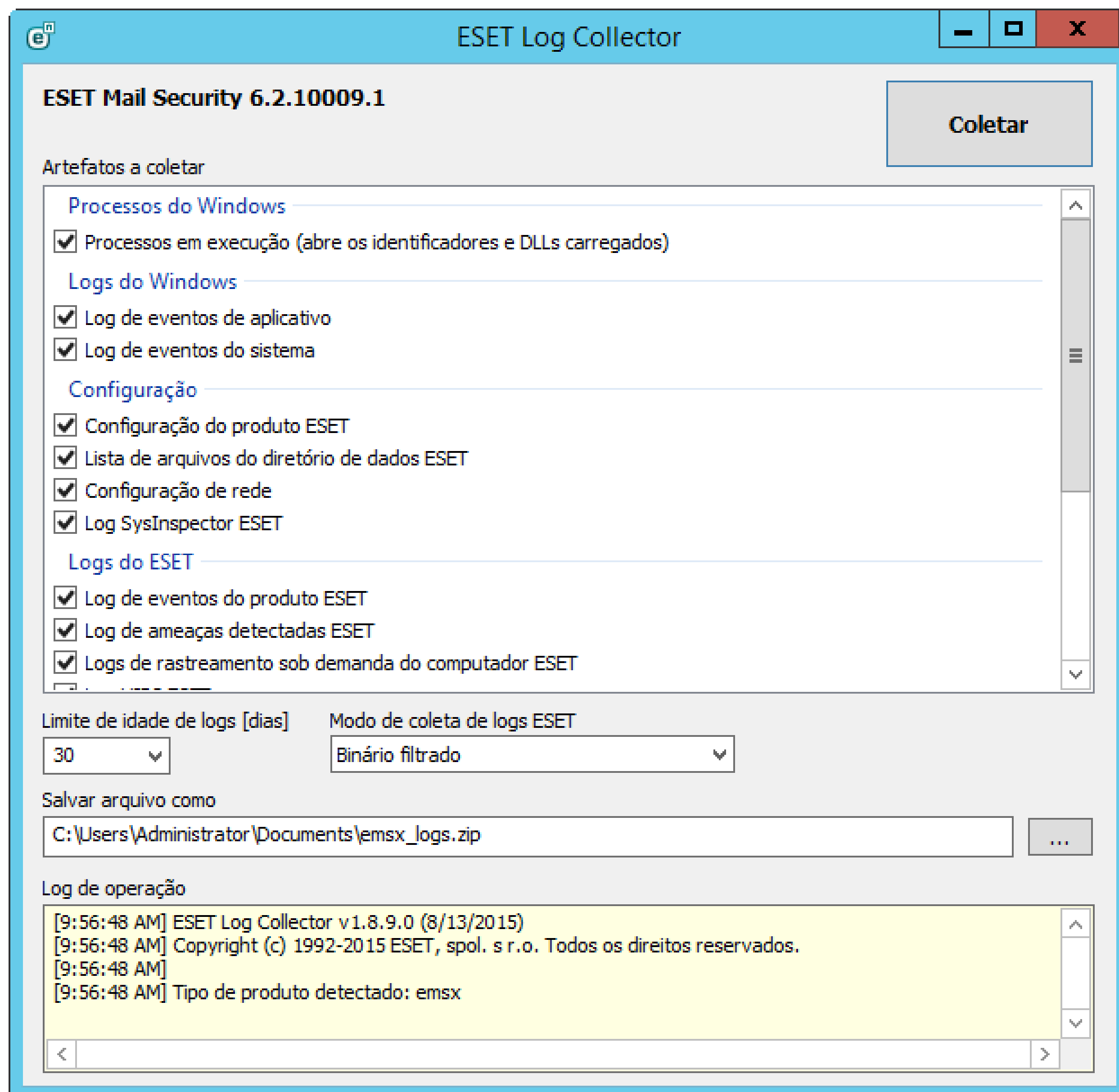
- **1 segundo** - O gráfico é atualizado a cada segundo e a linha de tempo cobre os últimos 10 minutos.
- **1 minuto (últimas 24 horas)** - O gráfico é atualizado a cada minuto e a linha de tempo cobre as últimas 24 horas.
- **1 hora (último mês)** - O gráfico é atualizado a cada hora e a linha de tempo cobre o último mês.
- **1 hora (mês selecionado)** - O gráfico é atualizado a cada hora e a linha de tempo cobre o último mês selecionado. Clique no botão **Alterar mês** para fazer outra seleção.

O eixo vertical do **Gráfico da atividade do sistema de arquivos** representa a quantidade de dados lidos (azul) e a quantidade de dados gravados (vermelho). Ambos os valores são fornecidos em KB (kilobytes)/MB/GB. Se você passar o mouse sobre os dados lidos ou sobre os dados gravados na legenda embaixo do gráfico, apenas os dados para esse tipo de atividade serão exibidos no gráfico.

4.7.3 ESET Log Collector

ESET Log Collector é um aplicativo que coleta automaticamente informações, como as configurações e relatórios do seu servidor, para ajudar a resolver problemas mais rapidamente. Quando houver um caso aberto com o Atendimento ao cliente ESET, poderá ser solicitado que você forneça relatórios de seu computador. O Coletor de relatório ESET facilitará sua coleta das informações necessárias.

ESET Log Collector pode ser acessado no menu principal clicando em **Ferramentas** > **Coletor de Relatório ESET**.



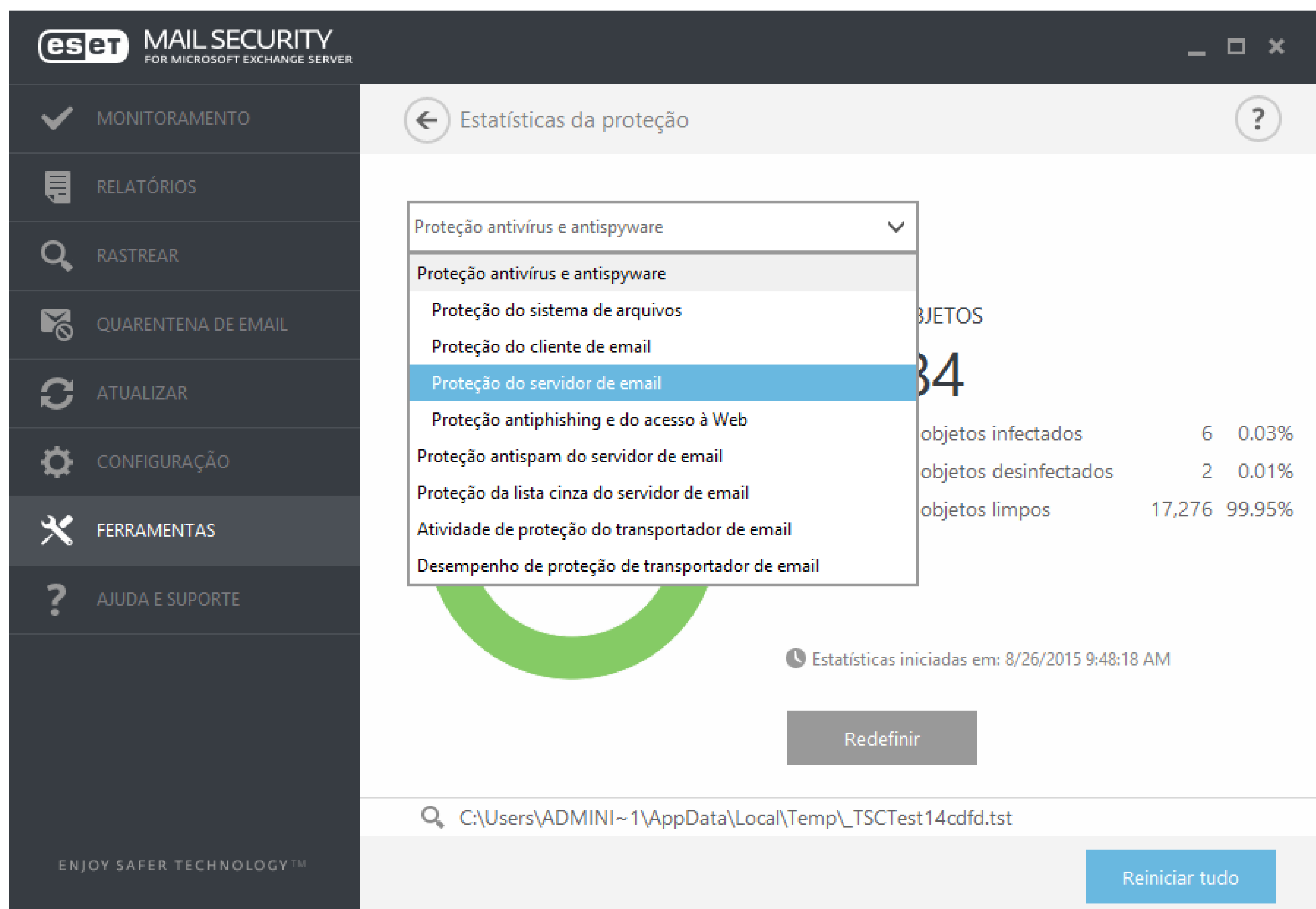
Selecione as caixas de seleção adequadas para os relatórios que você deseja coletar. Se você estiver inseguro em relação a qual selecionar, deixe todas as caixas de seleção marcadas (padrão). Especifique o local onde deseja salvar os arquivos e clique em **Salvar**. O nome do arquivo já está predefinido. Clique em **Coletar**.

Durante a coleta é possível ver a janela do relatório de operações na parte de baixo, para ver qual operação está sendo realizada no momento. Quando a coleta é concluída todos os arquivos que foram coletados e arquivados serão exibidos. Isso significa que a coleta foi bem sucedida, e o arquivo (por exemplo, `emsx_logs.zip`) foi salvo no local especificado.

Para mais informações sobre o ESET Log Collector e para uma lista dos arquivos que o ESET Log Collector realmente coleta, visite a [Base de conhecimento da ESET](#).

4.7.4 Estatísticas da proteção

Para exibir um gráfico de dados estatísticos sobre os módulos de proteção no ESET Mail Security, clique em **Ferramentas** > **Estatísticas da proteção**. Selecione o módulo de proteção desejado no menu suspenso **Estatísticas** para visualizar o gráfico e a legenda correspondentes. Passe o mouse sobre um item na legenda para exibir dados desse item no gráfico.



Os gráficos estatísticos a seguir estão disponíveis:

- **Proteção antivírus e antispyware** – Exibe o número geral de objetos infectados e limpos.
- **Proteção do sistema de arquivos** - Exibe apenas os objetos que foram lidos ou gravados no sistema de arquivos.
- **Proteção do cliente de email** - Exibe apenas os objetos que foram enviados ou recebidos pelos clientes de email.
- **Proteção do servidor de email** - Exibe estatísticas de antivírus e antispyware do servidor de email.
- **Proteção antiphishing e do acesso à Web** - Exibe apenas os objetos obtidos por download pelos navegadores da web.
- **Proteção antispam do servidor de email** - Exibe o histórico das estatísticas de antispam desde a última inicialização.
- **Proteção da lista cinza do servidor de email** - Inclui estatísticas antispam geradas usando o método de lista cinza.
- **Atividade de proteção do transportador de email** - exibe objetos verificados/bloqueados/excluídos pelo servidor de email.
- **Desempenho de proteção de transportador de email** - exibe dados processados pelo VSAPI/Agente de transporte, em B/s.
- **Atividade de proteção do banco de dados da caixa de entrada** - Exibe objetos processados pelo VSAPI (número de objetos **verificados, em quarentena** e **excluídos**).
- **Desempenho de proteção do banco de dados da caixa de entrada** - Exibe os dados processados por VSAPI (número de médias diferentes para **Hoje**, para os **Últimos 7 dias** e as médias **Desde a última redefinição**).

Ao lado dos gráficos de estatísticas, você pode ver o número total de objetos rastreados, infectados, que foram limpos e que estão limpos. Clique em **Redefinir** para limpar informações de estatísticas ou clique em **Redefinir tudo**

para limpar e remover todos os dados existentes.

4.7.5 Agrupamento

O **Agrupamento ESET** é uma infraestrutura de comunicação P2P da linha de produtos ESET para o Microsoft Windows Server.

Esta infraestrutura permite que os produtos de servidor da ESET se comuniquem uns com os outros e troquem dados como configurações e notificações, e também que sincronizem os dados necessários para a operação correta de um grupo de instâncias do produto. Um exemplo de tal grupo é um grupo de nós em um Agrupamento de Failover Windows ou Agrupamento de Balanceamento de Carga de Rede (NLB) com produto ESET instalado onde há necessidade de ter a mesma configuração do produto em todo o agrupamento. O Agrupamento ESET garante esta uniformidade entre instâncias.

A página de status do Agrupamento ESET pode ser acessada no menu principal em **Ferramentas** > **Agrupamento** quando configurada adequadamente, a página deve ter a seguinte aparência:

Para configurar o Agrupamento ESET, clique em **Assistente do agrupamento...** Para detalhes sobre como configurar o Agrupamento ESET usando o assistente, clique aqui.

Ao configurar o Agrupamento ESET existem duas formas de adicionar nós - automaticamente usando o Agrupamento de Failover Windows / Agrupamento NLB ou manualmente ao procurar computadores que estejam em um Grupo de trabalho ou em um Domínio.

Detectar automaticamente - detecta automaticamente nós que já fazem parte de um Agrupamento de Failover Windows / Agrupamento NLB e adiciona estes a um Agrupamento ESET
Procurar - É possível adicionar nós manualmente ao digitar os nomes do servidor (que sejam ou membros do mesmo Grupo de trabalho ou membros do mesmo Domínio)

OBSERVAÇÃO: O servidor não precisa fazer parte de um Agrupamento de Failover Windows / Agrupamento NLB para usar o recurso Agrupamento ESET. Um Agrupamento de Failover Windows ou Agrupamento NLB não precisa

estar instalado em seu ambiente para usar os agrupamentos ESET.

Assim que os nós tiverem sido adicionados ao seu Agrupamento ESET, a próxima etapa é a instalação do ESET Mail Security em cada nó. Isto é feito automaticamente durante a configuração do Agrupamento ESET.

Credenciais necessárias para a instalação remota do ESET Mail Security em outros nós de agrupamento:

- Cenário de Domínio - credenciais do administrador de domínio
- Cenário do grupo de trabalho - é preciso certificar-se de que todos os nós usam as mesmas credenciais de conta do administrador local

Em um Agrupamento ESET também é possível usar uma combinação de nós adicionados automaticamente como membros de um Agrupamento de Failover Windows / Agrupamento NLB existente e nós adicionados manualmente (desde que estejam no mesmo Domínio).

OBSERVAÇÃO: Não é possível combinar nós de Domínio com nós de Grupo de trabalho.

Outro requisito do Agrupamento ESET é que **Compartilhamento de arquivos e impressora** deve estar ativado no Firewall do Windows antes de fazer a instalação do ESET Mail Security nos nós do Agrupamento ESET.

O Agrupamento ESET pode ser desfeito facilmente clicando em **Destruir agrupamento**. Cada nó vai escrever um registro do seu relatório de eventos sobre o Agrupamento ESET ser destruído. Depois disso, todas as regas de firewall ESET são retiradas do Firewall do Windows. Nós anteriores serão revertidos no seu estado anterior e podem ser usados novamente em outro Agrupamento ESET se necessário.

OBSERVAÇÃO: A criação de Agrupamentos ESET entre o ESET Mail Security e o ESET File Security para Linux não é compatível.

Adicionar novos nós a um Agrupamento ESET existente pode ser feito a qualquer momento ao executar o **Assistente do agrupamento** da mesma forma descrita acima e aqui.

Veja a seção Agrupamento de trabalho para mais informações sobre a configuração de agrupamento ESET.

4.7.6 ESET Shell

O eShell (abreviação de ESET Shell) é a interface de linha de comando do ESET Mail Security. É uma alternativa à interface gráfica do usuário (GUI). O eShell possui todos os recursos e opções que a GUI geralmente oferece. O eShell permite configurar e administrar todo o programa sem usar a GUI.

Além de todas as funções e recursos disponíveis na GUI, o eShell também oferece a possibilidade de obter automação executando scripts para configurar, alterar configurações ou realizar uma ação. O eShell também pode ser útil para quem prefere usar linhas de comando em vez da GUI.

Há dois modos em que o eShell pode ser executado:

- Modo interativo: útil quando se deseja trabalhar com o eShell (não apenas executar um único comando), por exemplo para tarefas como alterar a configuração, visualizar relatórios, etc. Também é possível usar o modo interativo se ainda não estiver familiarizado com todos os comandos. O modo interativo facilita a navegação pelo eShell. Também exibe os comandos disponíveis que podem ser usados em este contexto específico.

- Comando único/Modo de lote: use este modo se deseja apenas executar um comando, sem entrar no modo interativo do eShell. Isso pode ser feito no prompt de comando do Windows, digitando `eshell` com os parâmetros apropriados. Por exemplo:

```
eshell get status
```

ou

```
eshell set antivirus status disabled
```

Para executar determinados comandos (como o segundo exemplo acima) no modo lote/script, existem algumas configurações que precisam ser configuradas antes. Caso contrário você receberá a mensagem **Acesso negado**. Isto acontece por motivos de segurança.

OBSERVAÇÃO: Para a funcionalidade completa, recomendamos abrir o eShell usando **Executar como administrador**. O mesmo é aplicável ao executar um comando único através do prompt de comando do Windows

(cmd). Abra o cmd usando **Executar como administrador**. Caso contrário você não poderá executar todos os comandos. Isso porque quando você abre o cmd ou o eShell usando uma conta que não a de administrador, você não terá permissões suficientes.

OBSERVAÇÃO: Para executar comandos do eShell no prompt de comando do Windows ou para executar arquivos em lote, é preciso fazer algumas configurações. Para mais informações sobre a execução de arquivos em lote, clique aqui.

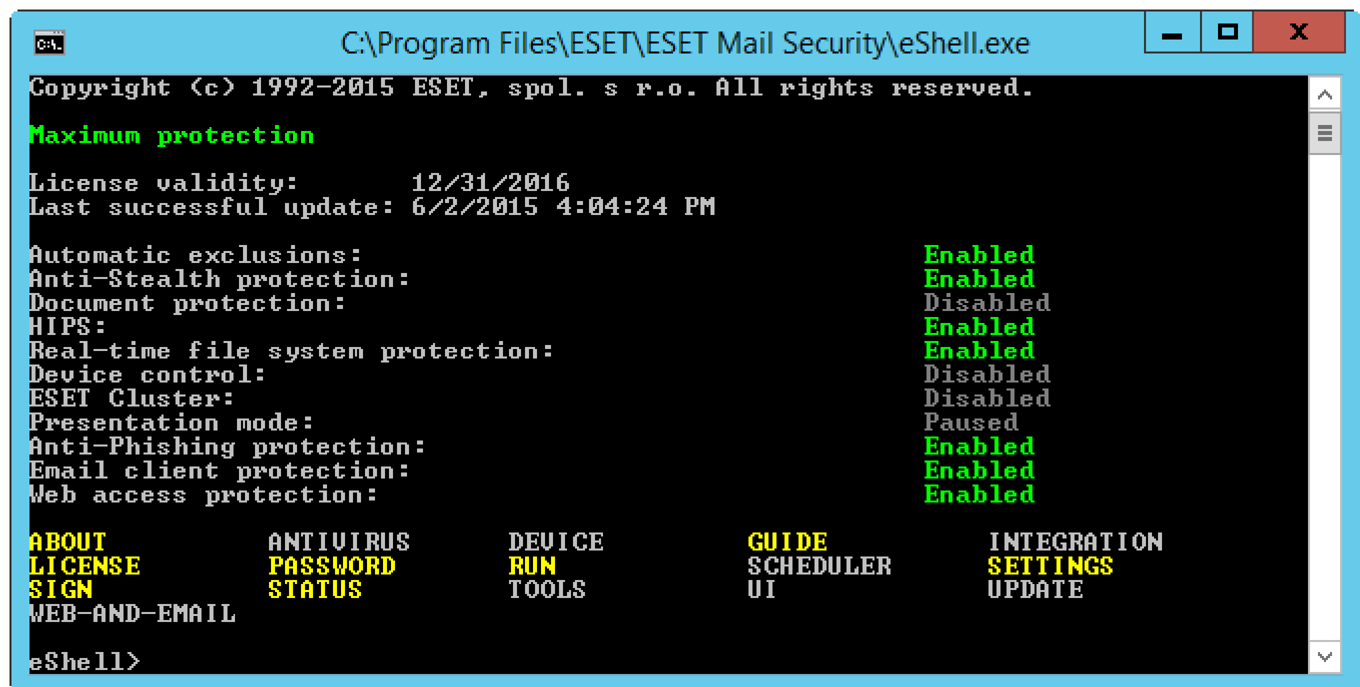
Para entrar no modo interativo do eShell, você pode usar um dos seguintes dois métodos:

- No menu Iniciar do Windows: **Iniciar** > **Todos os programas** > **ESET** > **ESET File Security** > **ESET shell**
- No prompt de comando do Windows, digite `eshell` e pressione a tecla Enter

Ao executar o eShell no modo interativo pela primeira vez, será exibida uma tela de primeira execução (guia).

OBSERVAÇÃO: Se quiser exibir esta tela no futuro, digite o comando `guide` . Ela exibe alguns exemplos básicos de como usar o eShell com Sintaxe, Prefixo, Caminho de comando, Formas abreviadas, Aliases, etc. Basicamente, é um guia rápido do eShell.

Na próxima vez que você executar o eShell, verá esta tela:



OBSERVAÇÃO: Os comandos não diferenciam maiúsculas de minúsculas. Você pode usar letras maiúsculas ou minúsculas e o comando será executado.

Personalizando o eShell

Você pode personalizar o eShell no contexto `ui eshell` . É possível configurar aliases, cores, idioma, política de execução para scripts, é possível escolher exibir comandos ocultos, e algumas outras configurações.

4.7.6.1 Uso

Sintaxe

Os comandos devem ser formatados na sintaxe correta para que funcionem e podem ser compostos de um prefixo, contexto, argumentos, opções, etc. Esta é a sintaxe geral utilizada em todo o eShell:

[<prefixo>] [<caminho de comando>] <comando> [<argumentos>]

Exemplo (isto ativa a proteção de documentos):

```
SET ANTIVIRUS DOCUMENT STATUS ENABLED
```

`SET` - um prefixo
`ANTIVIRUS DOCUMENT` - caminho para um comando específico, um contexto a que este comando pertence
`STATUS` - o comando em si
`ENABLED` - um argumento para o comando

Ao usar `?` com um argumento de comando, você verá a sintaxe para aquele comando específico. Por exemplo, `STATUS ?` exibirá a sintaxe do comando `STATUS` :

SINTAXE:

```
[get] | status
set status enabled | disabled
```

Observe que `[get]` está entre colchetes. Isso é o que denomina o prefixo `get` como padrão para o comando `status` . Isso significa que, ao executar o comando `status` sem especificar nenhum prefixo, será usado o prefixo padrão (que neste caso é `get status`). Use comandos sem prefixos para economizar tempo ao digitar. Normalmente `get` é o padrão para a maioria dos comandos, mas é necessário certificar-se qual é o prefixo padrão para um comando específico, e se é exatamente aquele que deseja executar.

i **OBSERVAÇÃO**: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

Prefixo/Operação

Um prefixo é uma operação. O comando `GET` fornecerá a informação de como um determinado recurso do ESET Mail Security está configurado ou exibirá um status (como `GET ANTIVIRUS STATUS` exibirá o status de proteção atual). O comando `SET` configurará o recurso ou alterará seu status (`SET ANTIVIRUS STATUS ENABLED` ativará a proteção).

Estes são os prefixos que o eShell permite que você use. Um comando pode ou não ser compatível com qualquer um dos prefixos:

`GET` - retorna as configurações/status atuais
`SET` - define o valor/status
`SELECT` - seleciona um item
`ADD` - adiciona um item
`REMOVE` - remove um item
`CLEAR` - remove todos os itens/arquivos
`START` - inicia uma ação
`STOP` - interrompe uma ação
`PAUSE` - pausa uma ação
`RESUME` - retoma uma ação
`RESTORE` - restaura as configurações/objeto/arquivo padrão
`SEND` - envia um objeto/arquivo
`IMPORT` - importa de um arquivo
`EXPORT` - exporta para um arquivo

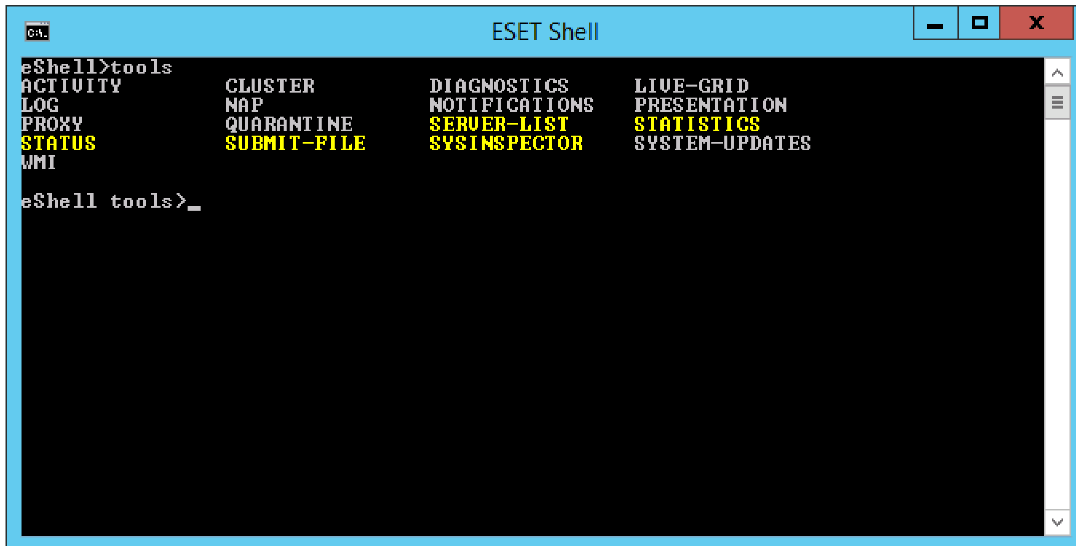
Prefixos como `GET` e `SET` são usados com vários comandos, mas alguns comandos, como `EXIT`, não usam prefixos.

Caminho de comando/Contexto

Os comandos são colocados em contextos que formam uma estrutura de árvore. O nível superior da árvore é a raiz. Ao executar o eShell, você está no nível raiz:

```
eShell>
```

Você pode executar o comando a partir daqui ou entrar um nome de contexto para navegar dentro da árvore. Por exemplo, ao entrar no contexto TOOLS , ele listará todos os comandos e subcontextos disponíveis ali.



Os que estão em amarelo são comandos que podem ser executados, os que estão em cinza são subcontextos nos quais você pode entrar. Um sub-contexto contém outros comandos.

Se precisar voltar para um nível superior, use .. (dois pontos). Por exemplo, se estiver em:

```
eShell antivirus startup>
```

digite .. e você será levado um nível acima para:

```
eShell antivirus>
```

Se quiser voltar à raiz de eShell antivirus startup> (que é dois níveis abaixo da raiz), digite apenas .. .. (dois pontos e dois pontos separados por espaço). Fazendo isso, você subirá dois níveis, que neste caso é a raiz. Use a barra invertida \ para voltar diretamente para a raiz a partir de qualquer nível, independentemente de onde estiver na árvore de contexto. Se quiser ir para um contexto determinado nos níveis superiores, apenas use o número adequado de .. para chegar ao nível desejado, mas use um espaço como separados. Por exemplo, se quiser subir três níveis, use .. .. ..

O caminho é relativo ao contexto atual. Se o comando estiver no contexto atual, não insira um caminho. Por exemplo, para executar GET ANTIVIRUS STATUS digite:

GET ANTIVIRUS STATUS - se estiver no contexto raiz (a linha de comando exibe eShell>)
GET STATUS - se estiver no contexto ANTIVÍRUS (a linha de comando exibe eShell antivirus>)
.. GET STATUS - se estiver no contexto ANTIVIRUS STARTUP (a linha de comando exibe eShell antivirus startup>)

OBSERVAÇÃO: Você pode usar um único . (ponto) em vez de dois .. porque um único ponto é uma abreviação de dois pontos. Por exemplo:

. GET STATUS - se estiver no contexto ANTIVIRUS STARTUP (a linha de comando exibe eShell antivirus startup>)

Argumento
Um argumento é uma ação realizada em um comando específico. Por exemplo, o comando CLEAN-LEVEL (localizado em ANTIVIRUS REALTIME ENGINE) pode ser usado com os seguintes argumentos:

no - Sem limpeza
normal - Limpeza normal
strict - Limpeza rígida

Outro exemplo são os argumentos ENABLED ou DESATIVADO, que são usados para ativar ou desativar determinados recursos.

Forma abreviada/Comandos encurtados
O eShell possibilita encurtar contextos, comandos e argumentos (desde que o argumento seja um alternador ou uma opção alternativa). Não é possível encurtar um prefixo ou um argumento que seja um valor concreto, como um

número, nome ou caminho.

Exemplos de forma abreviada:

```
set status enabled  => set stat en
add antivirus common scanner-excludes C:\path\file.ext => add ant com scann C:\path\file.ext
```

Se houver dois comandos ou contextos começando com as mesmas letras, por exemplo `ABOUT` e `ANTIVÍRUS`, e você digitar `A` como comando abreviado, o eShell não conseguirá decidir qual comando você deseja executar. Será exibida uma mensagem de erro e uma lista de comandos começando com "A" que poderão ser utilizados:

```
eShell>a
O seguinte comando não é exclusivo: a

Os seguintes comandos estão disponíveis neste contexto:
ABOUT - Exibe informações sobre o programa
ANTIVIRUS - Alterações ao contexto antivírus
```

Adicionar uma ou mais letras (p. ex. `AB` em vez de apenas `A`) o eShell executará o comando `ABOUT` , já que este é o único com estas letras.

OBSERVAÇÃO: Quando quiser ter certeza de que um comando será executado exatamente como deseja, recomendamos que não abrevie comandos, argumentos, etc. e use a forma completa. Dessa forma o comando será executado exatamente como deseja e isso evita erros indesejados. Especialmente no caso de arquivos/scripts em lote.

Preenchimento automático
É um novo recurso no eShell desde a versão 2.0. É muito similar ao preenchimento automático no prompt de comando do Windows. Enquanto o prompt de comando do Windows preenche caminhos de arquivo, o eShell preenche também comando, contexto e nome da operação. O preenchimento de argumento não é suportado. Ao digitar um comando, apenas pressione a tecla TAB para preencher ou para navegar nas variações disponíveis. Pressione SHIFT + TAB para fazer o ciclo voltando. A mistura de forma abreviada com o preenchimento automático não é suportada. Use um ou o outro. Por exemplo, ao digitar `antivir real scan` pressionar a tecla TAB não vai ter resultado nenhum. Em vez disso, digite `antivir` e depois pressione TAB para preencher com `antivírus`, continue digitando real + TAB e rastreamento + TAB. Então é possível navegar por todas as variações disponíveis: scan-create, scan-execute, scan-open, etc.

Aliases
Um alias é um nome alternativo que pode ser usado para executar um comando (desde que o comando tenha um alias atribuído a ele). Há alguns aliases padrão:

`(global) close` - sair
`(global) quit` - sair
`(global) bye` - sair
`warnlog` - eventos de relatório das ferramentas
`virlog` - detecções de relatório das ferramentas
`antivirus on-demand log` - rastreamento de relatório de ferramentas

"(global)" significa que o comando pode ser usado em qualquer lugar, independente do contexto atual. Um comando pode ter vários aliases atribuídos a ele, por exemplo o comando `EXIT` tem os aliases `CLOSE`, `QUIT` e `BYE`. Quando quiser sair do eShell, pode usar o comando `EXIT` ou qualquer um de seus aliases. Alias `VIRLOG` é um alias para o comando `DETECTIONS` , que está localizado no contexto `TOOLS LOG` . Portanto, as detecções do comando estão disponíveis no contexto `ROOT` , e são mais fáceis de acessar (não é necessário entrar nos contextos `TOOLS` e `LOG` , pode executá-lo diretamente de `ROOT`).

O eShell permite definir seus próprios aliases. O comando `ALIAS` pode ser encontrado em `UI ESHELL` .

Configurações protegidas por senha
As configurações do ESET Mail Security podem ser protegidas por uma senha. É possível definir a senha usando a interface gráfica do usuário ou eShell usando o comando `set ui access lock-password` . Você terá que inserir esta senha de forma interativa para certos comandos (como aqueles que podem alterar configurações ou modificar dados). Se você planeja trabalhar com o eShell por um período de tempo maior e não quer digitar a senha

repetidamente, é possível fazer com que o eShell lembre a senha usando o comando `set password`. Sua senha então será preenchida automaticamente para cada comando executado que precisar de senha. Ela é lembrada até que você saia do eShell, isso significa que será preciso usar o `set password` novamente quando iniciar uma nova sessão e quiser que o eShell lembre de sua senha.

Guia / Ajuda
Ao executar o comando `GUIDE` ou `HELP`, será exibida uma tela explicando como usar o eShell. Esse comando está disponível no contexto `ROOT` (`eShell>`).

Histórico de comandos
O eShell mantém um histórico dos comandos executados anteriormente. Isso se aplica apenas à sessão interativa atual do eShell. Quando você sair do eShell, o histórico do comando será removido. Use as teclas de seta para cima e para baixo em seu teclado para navegar pelo histórico. Quando encontrar o comando que está procurando, pode executá-lo ou alterá-lo sem ter que digitar todo o comando desde o início.

CLS/Limpar tela
O comando `CLS` pode ser usado para limpar a tela. Ele funciona da mesma forma que no prompt de comando do Windows ou interface de linha de comando similar.

EXIT/CLOSE/QUIT/BYE
Para fechar ou sair do eShell, você pode usar qualquer desses comandos (`EXIT`, `CLOSE`, `QUIT` ou `BYE`).

4.7.6.2 Comandos

Esta seção relaciona alguns comandos básicos do eShell com descrição como exemplo.

i **OBSERVAÇÃO**: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

Exemplo de comandos (contidos dentro do contexto ROOT):

ABOUT

Lista informações sobre o programa. Exibe o nome do produto instalado, o número da versão, os componentes instalados (incluindo número de versão de cada componente) e as informaçoes básicas sobre o servidor e o sistema operacional em que o ESET Mail Security está sendo executado.

CAMINHO DO CONTEXTO:

```
raiz
```

SENHA

Geralmente, para executar comandos protegidos por senha você é solicitado uma senha por motivos de segurança. Isso se aplica a comandos como os que desativam a proteção antivírus e os que podem afetar os recursos do ESET Mail Security. Será solicitada uma senha sempre que executar um desses comandos. Para evitar inserir uma senha a cada vez, você pode definir esta senha. Ela será lembrada pelo eShell e será usada automaticamente quando um comando protegido por senha for executado. Isso significa que não será preciso inseri-la.

i **OBSERVAÇÃO**: A senha definida funciona somente na sessão interativa atual do eShell. Quando você sair do eShell, esta senha definida será removida. Ao iniciar o eShell novamente, a senha precisará ser definida novamente.

Essa senha definida também é bastante útil ao executar arquivos/scripts em lote. Eis um exemplo de um arquivo em lote:

```
eshell start batch "&" set password plain <suasenha> "&" set status disabled
```

Este comando concatenado acima inicia um modo de lote, define a senha que será usada e desativa a proteção.

CAMINHO DO CONTEXTO:

```
raiz
```

SINTAXE:

`[get] | restore password`

`set password [plain <senha>]`

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou limpar a senha

`restore` - Limpar a senha

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`senha` - Senha

EXEMPLOS:

`set password plain <suasenha>` - Define uma senha que será usada para comandos protegidos por senha

`restore password` - Limpa a senha

EXEMPLOS:

`get password` - Use este comando para ver se a senha está configurada (isto apenas exibe asteriscos "*", não lista a senha em si), quando não forem exibidos asteriscos, significa que não há uma senha definida

`set password plain <suasenha>` - Use para definir a senha definida

`restore password` - Este comando limpa a senha definida

STATUS

Exibir informações sobre o status atual de proteção do ESET Mail Security (similar à GUI).

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

`[get] | restore status`

`set status disabled | enabled`

OPERAÇÕES:

`get` - Exibir o status da proteção antivírus

`set` - Ativar/Desativar a proteção antivírus

`restore` - Restaura as configurações padrão

ARGUMENTOS:

`disabled` - Desativar a proteção antivírus

`enabled` - Ativar a proteção antivírus

EXEMPLOS:

`get status` - Exibe o status de proteção atual

`set status disabled` - Desativa a proteção

`restore status` - Restaura a proteção às configurações padrão (ativada)

VIRLOG

Este é um alias do comando `DETECTIONS` . É útil para visualizar informações sobre infiltrações detectadas.

WARNLOG

Este é um alias do comando `EVENTS` . É útil para visualizar informações sobre vários eventos.

4.7.6.3 Arquivos em lote / Script

É possível usar o eShell como uma ferramenta de script potente para automação. Para usar um arquivo em lote com o eShell, crie um com o eShell e escreva comandos nele. Por exemplo:

```
eshell get antivirus status
```

Também é possível fazer comandos em cadeira, o que as vezes é necessário, por exemplo se você quiser obter um tipo de tarefa agendada em particular, digite o seguinte:

```
eshell select scheduler task 4 "&" get scheduler action
```

A seleção de um item (tarefa número 4 neste caso) normalmente é aplicável apenas à instância atual em execução do eShell. Se você fosse executar esses dois comandos um depois do outro, o segundo comando teria uma falha com o erro "Nenhuma tarefa selecionada ou a tarefa selecionada não existe mais".

Devido a motivos de segurança, a política de execução é definida como Script limitado por padrão. Isso permite que você use o eShell como uma ferramenta de monitoramento, mas não permite que você faça alterações de configuração no ESET Mail Security. Comandos que podem afetar a segurança, como desligar a proteção, receberão uma mensagem **Acesso negado**. Para ser capaz de executar esses comandos que fazem alterações na configuração, recomendamos usar arquivos em lote assinados.

Se, por algum motivo específico, você precisar ser capaz de alterar a configuração usando um único comando inserido manualmente no prompt de comando do Windows, você terá que conceder acesso total ao eShell (não recomendável). Para conceder acesso total, use o comando `ui eshell shell-execution-policy` no modo Interativo do próprio eShell, ou faça isso através da interface gráfica do usuário em **Configuração avançada** > **Interface de usuário** > ESET Shell.

Arquivos em lote assinados
O eShell permite proteger arquivo em lote comuns (*.bat) com uma assinatura. Scripts são assinados com a mesma senha usada para proteção de configurações. Para assinar um script é preciso primeiro ativar a proteção de configurações. Isso pode ser feito através da interface gráfica do usuário, ou de dentro do eShell usando o comando `set ui access lock-password` . Quando a senha de proteção de configurações estiver definida, você pode começar a assinar os arquivos em lote.

Para assinar um arquivo em lote, execute `sign <script.bat>` no seu contexto raiz do eShell, onde *script.bat* é o caminho para o script que você deseja assinar. Digite e confirme a senha que será usada para assinatura. Esta senha deve combinar com a senha de proteção de configurações. A assinatura é colocada no final do arquivo em lote na forma de um comentário. Caso este script tenha sido assinado anteriormente, a assinatura será substituída pela nova.

i **OBSERVAÇÃO**: Ao modificar um arquivo em lote assinado anteriormente, ele precisa ser assinado novamente.

i **OBSERVAÇÃO**: Se você alterar a senha de proteção de configurações é preciso assinar todos os scripts novamente, caso contrário os scripts vão ter uma falha de execução no momento em que você tiver alterado a senha de proteção de configurações. Isso acontece porque a senha inserida ao assinar um script deve ser correspondente com a senha de proteção de configurações no sistema de destino.

Para executar um arquivo em lote assinado no prompt de comando do Windows ou como uma tarefa agendada, use o comando a seguir:

```
eshell run <script.bat>
```

Onde script.bat é o caminho para o arquivo em lote. Por exemplo `eshell run d:\myeshellscript.bat`

4.7.7 ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o computador, coleta informações detalhadas sobre os componentes do sistema, como os drivers e aplicativos instalados, as conexões de rede ou entradas de registo importantes, e avalia o nível de risco de cada componente. Essas informações podem ajudar a determinar a causa do comportamento suspeito do sistema, que pode ser devido a incompatibilidade de software ou hardware ou infecção por malware.

A janela do ESET SysInspector exibe as seguintes informações sobre os relatórios criados:

- **Hora** - A hora de criação do relatório.
- **Comentário** - Um comentário curto.
- **Usuário** - O nome do usuário que criou o log.
- **Status** - O status de criação do relatório.

As seguintes ações estão disponíveis:

- **Abrir** - Abre um relatório criado. Isto também pode ser feito clicando com o botão direito no relatório criado e selecionando **Exibir** no menu de contexto.
- **Comparar** - Compara dois relatórios existentes.
- **Criar** - Cria um novo relatório. Aguarde até que o relatório do ESET SysInspector seja concluído (**Status** exibido como Criado).
- **Excluir** - Remove os relatórios selecionados da lista.

Após clicar com o botão direito em um ou mais relatórios selecionados, as seguintes opções estarão disponíveis no menu de contexto:

- **Mostrar** - Abre o relatório selecionado no ESET SysInspector (igual a clicar duas vezes em um relatório).
- **Criar** - Cria um novo relatório. Aguarde até que o relatório do ESET SysInspector seja concluído (**status** exibido como Criado)
- **Excluir tudo** - Exclui todos os logs.
- **Exportar** - Exporta o relatório para um arquivo *.xml* ou *.xml* compactado.

4.7.7.1 Criar um snapshot do status do computador

Digite um breve comentário que descreve o log a ser criado e clique no botão **Adicionar**. Aguarde até que o relatório do ESET SysInspector seja concluído (status Criado). A criação de relatórios pode levar algum tempo, dependendo da sua configuração de hardware e dados do sistema.

4.7.7.2 ESET SysInspector

4.7.7.2.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada em soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões são idênticas em função e têm os mesmos controles de programa. A única diferença é como os resultados são gerenciados. As versões integrada e separada permitem exportar snapshots do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os snapshots do sistema diretamente em **Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator).

Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

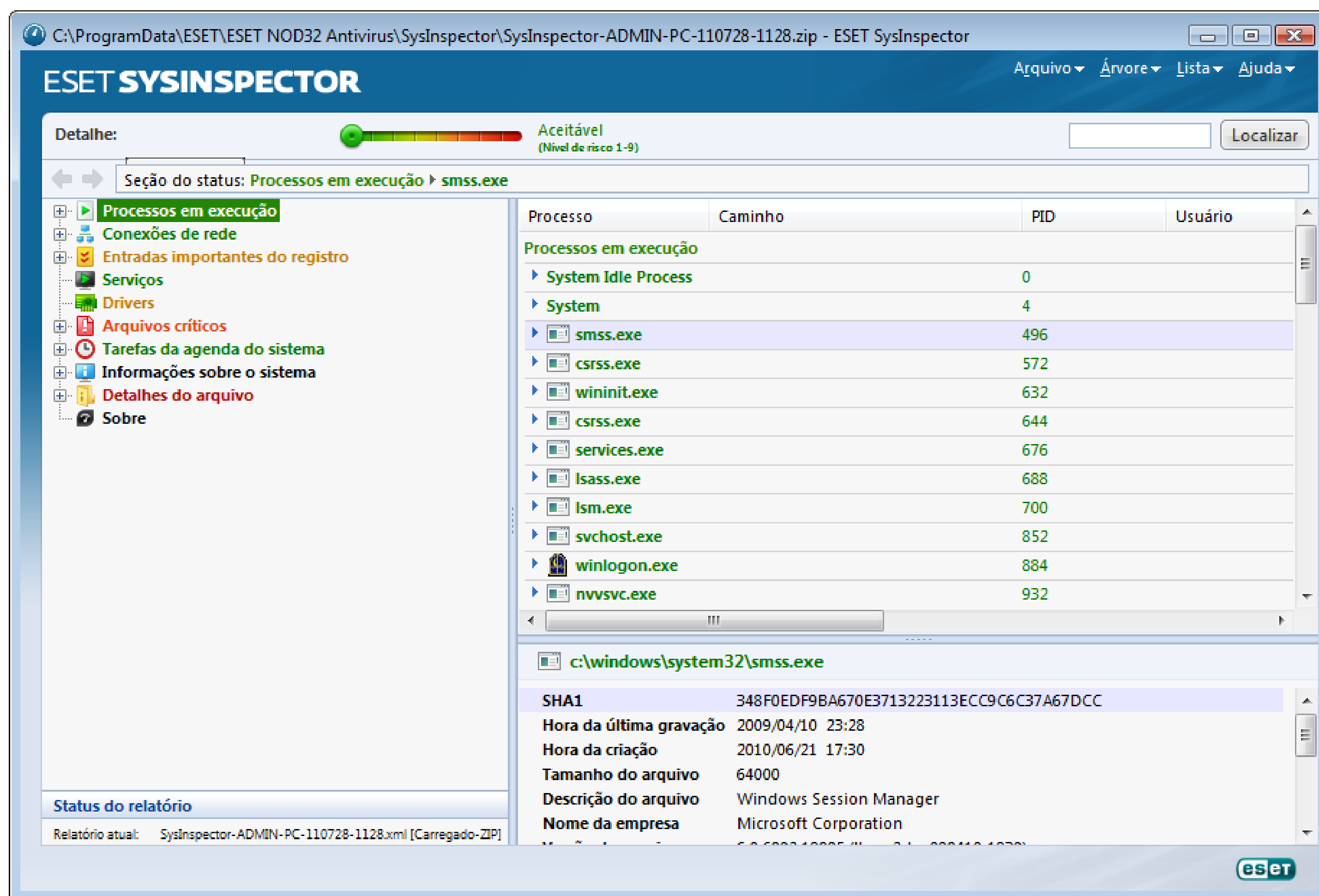
4.7.7.2.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo *SysInspector.exe* obtido por download no site da ESET.

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos, dependendo do hardware e dos dados a serem coletados.

4.7.7.2.2 Interface do usuário e uso do aplicativo

Para facilitar o uso, a janela principal é dividida em quatro seções: Controles do programa, localizados na parte superior da janela principal, a janela de navegação à esquerda, a janela de descrição à direita e no centro, e a janela de detalhes à direita, na parte inferior da janela principal. A seção Status do relatório lista os parâmetros básicos de um relatório (filtro usado, tipo do filtro, se o relatório é resultado de uma comparação, etc.).



4.7.7.2.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um relatório armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um relatório **Adequado para envio**. Neste formulário, o relatório omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente simplesmente arrastando e soltando-os na janela principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela principal, para que seja mais fácil trabalhar com estas informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe menos detalhes usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para solucionar problemas muito específicos.

Filtragem de itens

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver totalmente à esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante totalmente à direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens classificados como risco 6 a 9 podem ser um risco à segurança. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrar esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Pesquisar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, verifique se os arquivos são realmente perigosos ou desnecessários.

4.7.7.2.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou, como alternativa, clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do relatório. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo e o nível de risco do arquivo.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados 24 horas por dia, 7 dias por semana e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas frequentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como Serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de tarefas do Windows em um intervalo/horário especificado.

Informações do sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas e direitos do usuário.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista de módulos do programa.

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O	abre o relatório existente
Ctrl+S	salva os relatórios criados

Gerar

Ctrl+G	gera um instantâneo padrão do status do computador
Ctrl+H	gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O	aceitável, nível de risco 1-9, os itens são exibidos
2	aceitável, nível de risco 2-9, os itens são exibidos
3	aceitável, nível de risco 3-9, os itens são exibidos
4, U	desconhecido, nível de risco 4-9, os itens são exibidos
5	desconhecido, nível de risco 5-9, os itens são exibidos
6	desconhecido, nível de risco 6-9, os itens são exibidos
7, B	perigoso, nível de risco 7-9, os itens são exibidos
8	perigoso, nível de risco 8-9, os itens são exibidos
9	perigoso, nível de risco 9, os itens são exibidos
-	diminui o nível de risco
+	aumenta o nível de risco
Ctrl+9	modo de filtragem, nível igual ou superior
Ctrl+0	modo de filtragem, somente nível igual

Exibir

Ctrl+5	exibição por fornecedor, todos os fornecedores
Ctrl+6	exibição por fornecedor, somente Microsoft
Ctrl+7	exibição por fornecedor, todos os outros fornecedores
Ctrl+3	exibe detalhes completos
Ctrl+2	exibe detalhes da mídia
Ctrl+1	exibição básica
Backspace	move um passo para trás
Espaço	move um passo para a frente
Ctrl+W	expande a árvore
Ctrl+Q	recolhe a árvore

Outros controles

Ctrl+T	vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	exibe informações básicas sobre um item
Ctrl+A	exibe informações completas sobre um item
Ctrl+C	copia a árvore do item atual
Ctrl+X	copia itens

Ctrl+B	localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	abre a entrada correspondente no editor do registro
Ctrl+Z	copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	alterna para o campo de pesquisa
Ctrl+D	fecha os resultados da pesquisa
Ctrl+E	executa script de serviços

Comparação

Ctrl+Alt+O	abre o relatório original/comparativo
Ctrl+Alt+R	cancela a comparação
Ctrl+Alt+1	exibe todos os itens
Ctrl+Alt+2	exibe apenas os itens adicionados; o relatório mostrará os itens presentes no relatório atual
Ctrl+Alt+3	exibe apenas os itens removidos; o relatório mostrará os itens presentes no relatório anterior
Ctrl+Alt+4	exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	exibe apenas as diferenças entre os relatórios
Ctrl+Alt+C	exibe a comparação
Ctrl+Alt+N	exibe o relatório atual
Ctrl+Alt+P	exibe o relatório anterior

Diversos

F1	exibe a ajuda
Alt+F4	fecha o programa
Alt+Shift+F4	fecha o programa sem perguntar
Ctrl+I	estatísticas de relatórios

4.7.7.2.2.3 Comparar

O recurso Comparar permite que o usuário compare dois relatórios existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os relatórios. Ele é adequado se você deseja manter controle das alterações no sistema; é uma ferramenta útil para detectar a atividade de código malicioso.

Após ser iniciado, o aplicativo criará um novo relatório que será exibido em uma nova janela. Navegue até **Arquivo** > **Salvar relatório** para salvar um relatório em um arquivo. Os relatórios podem ser abertos e visualizados posteriormente. Para abrir um relatório existente, utilize o menu **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um relatório de cada vez.

O benefício de comparar dois relatórios é que você pode visualizar um relatório ativo no momento e um relatório salvo em um arquivo. Para comparar relatórios, utilize a opção **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O relatório selecionado será comparado com o relatório ativo na janela principal do programa. O relatório comparativo exibirá apenas as diferenças entre esses dois relatórios.

OBSERVAÇÃO: Caso compare dois relatórios, selecione **Arquivo** > **Salvar relatório** e salve-o como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir este arquivo posteriormente, os relatórios contidos serão comparados automaticamente.

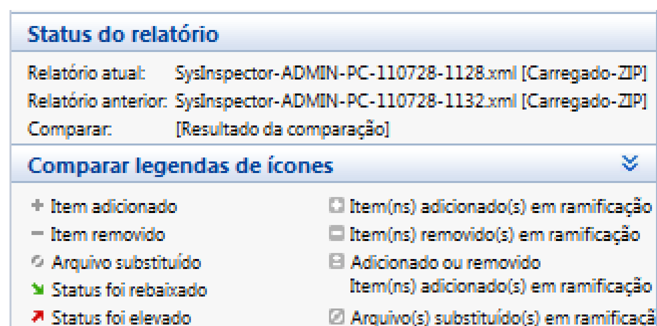
Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os relatórios comparados.

Os itens marcados por um - apenas podem ser encontrados no relatório ativo e não estavam presentes no relatório comparativo aberto. Os itens marcados por um + estavam presentes apenas no relatório aberto e estavam ausentes no relatório ativo.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- novo valor, não presente no relatório anterior
- a seção de estrutura em árvore contém novos valores
- valor removido, presente apenas no relatório anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no relatório anterior
- o nível de risco aumentou / era menor no relatório anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos relatórios que estão sendo comparados.



Qualquer relatório comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois relatórios, navegue até **Arquivo** > **Comparar relatórios**. O programa criará um relatório comparativo mostrando as diferenças entre os relatórios.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

4.7.7.2.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar um relatório diretamente a partir da linha de comando sem executar a GUI
/privacy	gerar um relatório excluindo informações confidenciais
/zip	armazenar o relatório resultante diretamente no disco em um arquivo compactado
/silent	ocultar a exibição da barra de progresso da geração de relatórios
/help, /?	exibir informações sobre os parâmetros da linha de comando

Exemplos

Para carregar um relatório específico diretamente no navegador, use: *SysInspector.exe "c:\clientlog.xml"*
Para gerar um relatório em um local atual, use: *SysInspector.exe /gen*
Para gerar um relatório em uma pasta específica, use: *SysInspector.exe /gen="c:\folder\"*
Para gerar um relatório em um arquivo/local específico, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Para gerar um relatório que exclua informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Para comparar dois relatórios, use: *SysInspector.exe "current.xml" "original.xml"*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

4.7.7.2.4 Script de serviços

O script de serviços é uma ferramenta que oferece ajuda a clientes que usam o ESET SysInspector, removendo facilmente objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o relatório modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As alterações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador esteja infectado por um vírus que não é detectado pelo seu programa antivírus, siga as instruções passo-a-passo a seguir:

- Execute o ESET SysInspector para gerar um novo snapshot do sistema.
- Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Ctrl e selecione o último item para marcar todos os itens.
- Clique com o botão direito nos objetos selecionados e selecione a opção do menu de contexto **Exportar as seções selecionadas para script de serviços**.
- Os objetos selecionados serão exportados para um novo relatório.
- Esta é a etapa mais crucial de todo o procedimento: abra o novo relatório e altere o atributo – para + para todos os objetos que desejar remover. Certifique-se de não marcar nenhum arquivo/objeto importante do sistema operacional.
- Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o seu script.
- Clique em **OK** para executar o script.

4.7.7.2.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector. No menu de contexto, selecione a opção **Exportar todas as seções para script de serviços** ou a opção **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois relatórios estiverem sendo comparados.

4.7.7.2.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, há informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do relatório (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando você executar o script, os drivers selecionados serão interrompidos. Observe que alguns drivers não permitirão eles mesmos a interrupção.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos críticos para o sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos, ou serão restaurados seus valores padrão originais.

4.7.7.2.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma caixa de diálogo confirmará que o script foi executado com sucesso.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

4.7.7.2.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um relatório?

O ESET SysInspector pode criar um relatório da configuração do computador. Para salvar um relatório, selecione **Arquivo** > **Salvar relatório** no menu principal. Os relatórios são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\My Documents*, com uma convenção de nomenclatura de arquivos de "SysInpsector-%NOMECOMPUTADOR%-AAMMDD-HHMM.XML". Você pode alterar o local e o nome do relatório para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o relatório do ESET SysInspector?

Para visualizar um relatório criado pelo ESET SysInspector, execute o programa e selecione **Arquivo** > **Abrir relatório** no menu principal. Você também pode arrastar e soltar relatórios no aplicativo ESET SysInspector. Se você precisar visualizar os relatórios do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os relatórios para visualização. Por motivo de segurança, os Windows Vista/7 podem não permitir operações de arrastar e soltar entre janelas que tenham

permissões de segurança diferentes.

Há uma especificação disponível para o formato do relatório? E um SDK?

Atualmente, não há uma especificação para o relatório nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 - Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro deles.

Um nível de risco "6 – Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles também podem examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporta como um rootkit, o usuário será exposto ao risco de danos ou roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validando usando essas informações. Se uma assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado. Se o arquivo CAT pertinente for encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em *C:\Arquivos de Programas\Windows NT*. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que aponta para *C:\Arquivos de Programas\Windows NT\hypertrm.exe* (o executável principal do aplicativo HyperTerminal) e o *sp4.cat* é digitalmente assinado pela Microsoft.

4.7.8 ESET SysRescue Live

o ESET SysRescue Live é um utilitário que permite criar um disco inicializável que contém uma das soluções ESET Security - ESET NOD32 Antivirus, ESET Smart Security ou certos produtos feitos para servidor. A principal vantagem do ESET SysRescue Live é o fato de a solução ESET Security ser executada de maneira independente do sistema operacional host, mas tem um acesso direto ao disco e ao sistema de arquivos. Isso possibilita remover as infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

4.7.9 Agenda

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis para serem utilizados durante a execução de uma tarefa.

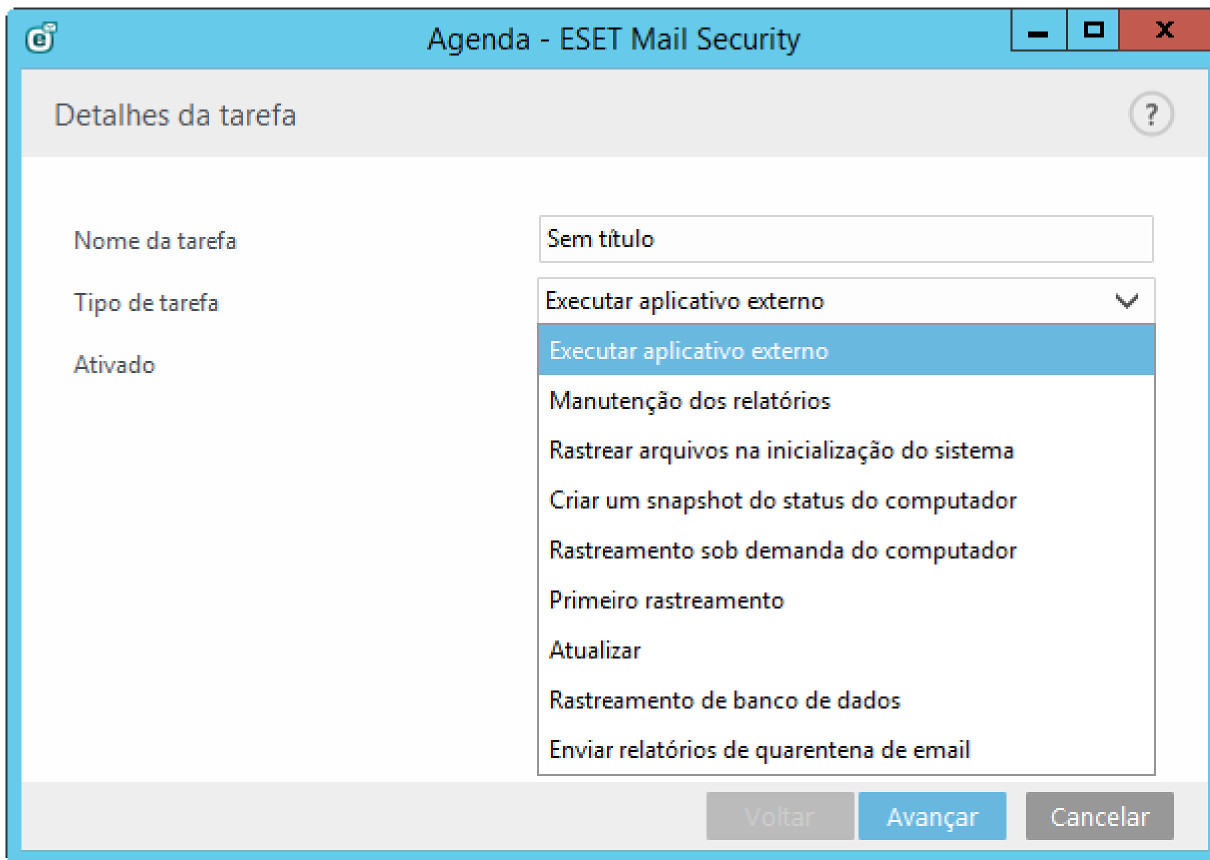
A Agenda pode ser acessada na janela principal do programa do ESET Mail Security em **Ferramentas** > **Agenda**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

A Agenda serve para agendar as seguintes tarefas: atualização da base de dados das assinaturas de vírus, tarefa de rastreamento, rastreamento de arquivos na inicialização do sistema e manutenção do relatório. Você pode adicionar ou excluir tarefas diretamente da janela principal da Agenda (clique em **Adicionar tarefa** ou **Excluir**). Clique com o botão direito em qualquer parte na janela de Agenda para realizar as seguintes ações: exibir informações detalhadas, executar a tarefa imediatamente, adicionar uma nova tarefa ou excluir uma tarefa existente. Use as caixas de seleção no início de cada entrada para ativar/desativar as tarefas.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção dos relatórios**
- **Atualização automática de rotina**
- **Atualizar automaticamente após a conexão dial-up ter sido estabelecida**
- **Atualizar automaticamente após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após logon do usuário)
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após atualização bem sucedida do banco de dados de assinatura de vírus)
- **Primeiro rastreamento automático**

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar** ou selecione a tarefa que deseja modificar e clique em **Editar**.



Adicionar uma nova tarefa

1. Clique em **Adicionar tarefa** na parte inferior da janela.

2. Escolha um nome para a tarefa.

3. Selecione a tarefa desejada no menu suspenso:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de relatório** - Os relatórios também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos relatórios para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um rastreamento do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - Por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização**- Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

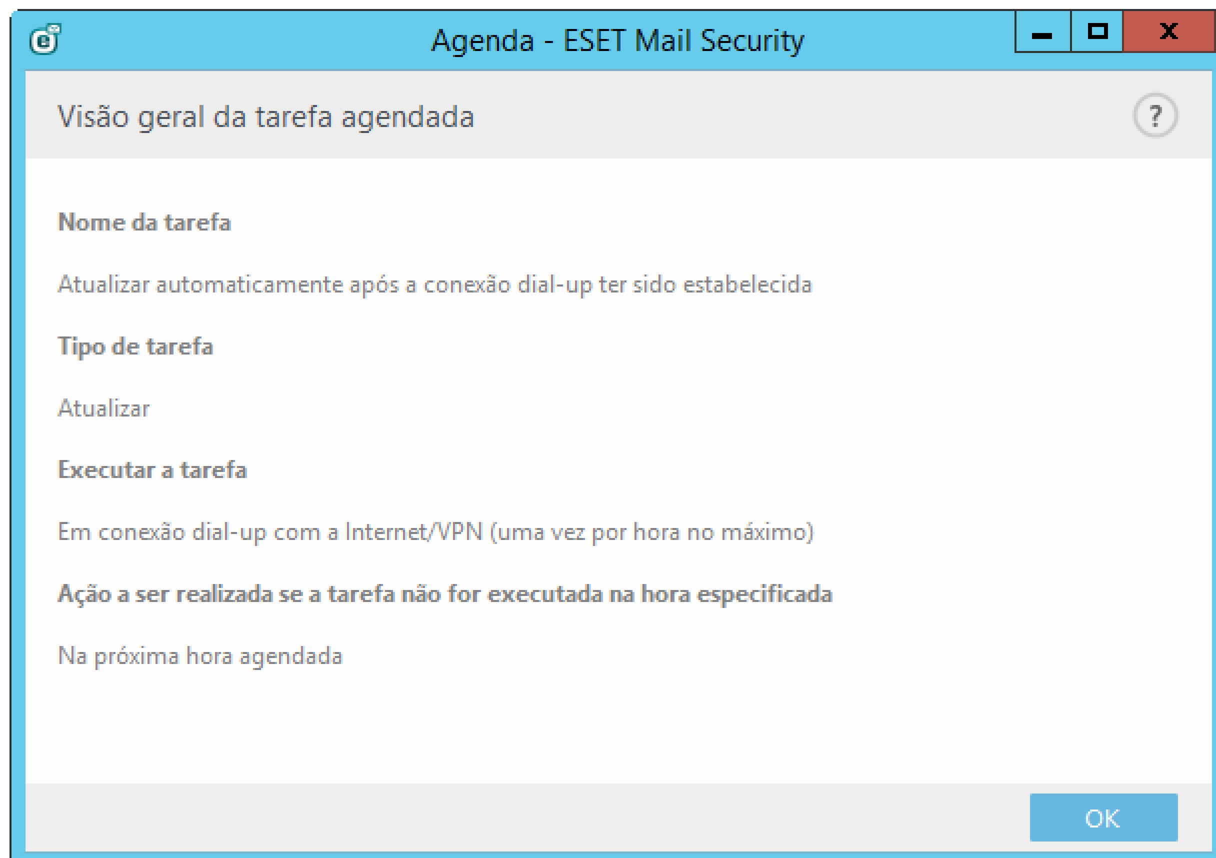
4. Clique em **Ativado** se quiser ativar a tarefa (você pode fazer isso posteriormente marcando/desmarcando a caixa de seleção na lista de tarefas agendadas), clique em **Avançar** e selecione uma das opções de tempo:

- **Uma vez** - A tarefa será realizada na data e hora predefinidas.
- **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado.
- **Diariamente** - A tarefa será executada repetidamente todos os dias no horário especificado.
- **Semanalmente** - A tarefa será realizada na data e hora selecionadas.
- **Evento disparado**- A tarefa será realizada após um evento especificado.

5. Selecione **Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada novamente:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução**)

Clique com o botão direito em uma tarefa e clique em **Exibir detalhes da tarefa** no menu de contexto para ver informações sobre a tarefa.



4.7.10 Enviar amostras para análise

A caixa de diálogo de envio de amostras permite enviar um arquivo ou site para a ESET para fins de análise e pode ser acessada em **Ferramentas** > **Enviar amostra para análise**. Se você detectar um arquivo com comportamento suspeito no seu computador ou um site suspeito na internet, poderá enviá-lo para o Laboratório de vírus da ESET para análise. Se for detectado que o arquivo é um aplicativo ou site malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Como alternativa, você pode enviar o arquivo por email. Para isso, compacte o(s) arquivo(s) usando um programa como WinRAR ou WinZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o arquivo (por exemplo, o site do qual fez o download).

Enviar arquivo para análise - ESET Mail Security

Selecionar amostra para análise

Motivo para envio do arquivo:

Arquivo suspeito

Arquivo:

"C:\Users\Administrator\Desktop\Sceenshots\EMSX.xml"

Email de contato:

O email de contato é enviado junto com arquivos suspeitos para o ESET e poderá ser usado para contatá-lo se forem necessárias mais informações. Fornecer o email é opcional e normalmente você não irá receber uma resposta nossa.

Voltar | Avançar | Cancelar

OBSERVAÇÃO: antes de enviar uma amostra para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o arquivo ou site não foi detectado
- o arquivo ou site foi detectado incorretamente como uma ameaça

Você não receberá uma resposta, a não ser que mais informações sejam necessárias para a análise.

Selecione a descrição no menu suspenso **Motivo para envio da amostra** mais adequada à sua mensagem:

- **Arquivo suspeito**
- **Site suspeito** (um site que está infectado por algum malware)
- **Arquivo falso positivo** (arquivo que é detectado como uma infecção, mas que não está infectado)
- **Site falso positivo**
- **Outros**

Arquivo/Site - O caminho do arquivo ou site que você pretende enviar.

Email de contato - O email de contato é enviado junto com arquivos suspeitos para a ESET e pode ser utilizado para contatar você se informações adicionais sobre os arquivos suspeitos forem necessárias para análise. É opcional inserir um email de contato. Você não obterá uma resposta da ESET, a menos que mais informações sejam necessárias, pois a cada dia os nossos servidores recebem milhares de arquivos, o que torna impossível responder a todos os envios.

4.7.10.1 Arquivo suspeito

Sinais e sintomas de infecção por malware observados - Insira uma descrição do comportamento do arquivo suspeito observado em seu computador.

Origem do arquivo (endereço URL ou fabricante) - Informe a origem do arquivo (source) e como ele foi encontrado.

Observações e informações adicionais - Aqui você pode inserir informações adicionais ou uma descrição que ajudará no processo de identificação do arquivo suspeito.

i **OBSERVAÇÃO:** O primeiro parâmetro - **Sinais e sintomas de infecção por malware observados** - é obrigatório, mas fornecer informações adicionais ajudará de maneira significativa nossos laboratórios a identificar e processar as amostras.

4.7.10.2 Site suspeito

Selecione uma das opções a seguir no menu suspenso **Qual o problema com o site**:

- **Infectado** - Um site que contenha vírus ou outro malware distribuído por vários métodos.
- **Roubo de identidade** - é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN e outros. Leia mais sobre esse tipo de ataque no glossário.
- **Fraude** - uma fraude ou site fraudulento.
- Selecione **Outro** se as opções acima não estiverem relacionadas ao site que você vai enviar.

Observações e informações adicionais - Aqui você pode inserir informações adicionais ou uma descrição que ajudará a analisar o site suspeito.

4.7.10.3 Arquivo falso positivo

Solicitamos que você envie os arquivos que foram detectados como uma infecção, mas não estão infectados, para melhorar nosso motor de antivírus e antispyware e ajudar na proteção de outros. Os casos de arquivos falsos positivos (FP) podem ocorrer quando um padrão de um arquivo corresponde ao mesmo padrão contido em um banco de dados de assinatura de vírus.

Nome e versão do aplicativo - Nome do programa e sua versão (por exemplo, número, alias ou código).

Origem do arquivo (endereço URL ou fabricante) - Informe a origem do arquivo (source) e como ele foi encontrado.

Propósito dos aplicativos - Descrição geral do aplicativo, tipo de um aplicativo (por exemplo, navegador, media player etc.) e sua funcionalidade.

Observações e informações adicionais - Aqui você pode adicionar descrições ou informações adicionais que ajudarão no processamento do arquivo suspeito.

i **OBSERVAÇÃO:** O comando os primeiros três parâmetros são necessários para identificar os aplicativos legítimos e distingui-los do código malicioso. Forneça informações adicionais para ajudar nossos laboratórios de maneira significativa a processar e a identificar as amostras.

4.7.10.4 Site falso positivo

Encorajamos que você envie os sites que foram detectados como infectados, scam ou sites de roubo de identidade, mas não são. Os casos de arquivos falsos positivos (FP) podem ocorrer quando um padrão de um arquivo corresponde ao mesmo padrão contido em um banco de dados de assinatura de vírus. Forneça o site para melhorar nosso motor de antivírus e antiphishing e ajudar os outros a estarem protegidos.

Observações e informações adicionais - Aqui você pode adicionar descrições ou informações adicionais que ajudarão no processamento do arquivo suspeito.

4.7.10.5 Outros

Utilize este formulário se o arquivo não puder ser categorizado como um **Arquivo suspeito** ou **Falso positivo**.

Motivo para envio do arquivo - Insira uma descrição detalhada e o motivo pelo qual está enviando o arquivo.

4.7.11 Quarentena

A principal função da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Mail Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de vírus da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, objeto adicionado pelo usuário) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças).

Colocação de arquivos em quarentena

o ESET Mail Security coloca automaticamente os arquivos excluídos em quarentena (se você não desativou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena.** O arquivo em quarentena será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena**.

Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Para isso, utilize o recurso **Restaurar**, que está disponível no menu de contexto, clicando com o botão direito do mouse no arquivo desejado, na janela Quarentena. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, a opção **Restaurar e excluir do rastreamento** estará disponível. Leia mais sobre esse tipo de aplicativo no glossário. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO: Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de vírus da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

4.8 Ajuda e suporte

O ESET Mail Security contém ferramentas de solução de problemas e informações de suporte que o ajudarão a solucionar eventuais problemas.

Ajuda

- **Pesquisar na Base de conhecimento ESET** - A Base de conhecimento da ESET contém as respostas à maioria das perguntas mais frequentes e as soluções recomendadas para diversos problemas. A atualização regular feita pelos especialistas técnicos da ESET tornam a base de conhecimento a ferramenta mais poderosa para a solução de diversos tipos de problemas.
- **Abrir ajuda** - Clique nesse link para iniciar as páginas de ajuda do ESET Mail Security.
- **Encontrar uma solução rápida** - Selecione para encontrar soluções para os problemas mais frequentemente encontrados. Recomendamos que você leia toda esta seção antes de contatar o suporte técnico.

Atendimento ao cliente

- **Enviar solicitação de suporte** - Se não puder encontrar a resposta para o seu problema, você pode usar o formulário no site da ESET para entrar em contato rapidamente com o nosso departamento de Atendimento ao Cliente.

Ferramentas de suporte

Enciclopédia de ameaças - Links para a Enciclopédia de ameaças da ESET, que contém informações sobre os perigos e os sinais de diferentes tipos de infiltração.

Histórico do banco de dados de assinatura de vírus - Links para o radar ESET Vírus, que contém informações sobre versões do banco de dados de assinatura de vírus da ESET.

Limpador especializado - Este limpador automaticamente identifica e remove infecções de malware comuns, para mais informações visite este artigo na Base de conhecimento ESET.

Informações do produto e licença

- **Sobre o ESET Mail Security -**Exibe informações sobre sua cópia do ESET Mail Security.
- Gerenciar licenças - Clique para iniciar a janela Ativação do produto. Selecione um dos métodos disponíveis para ativar o ESET Mail Security. Para obter mais informações, consulte Como ativar o ESET Mail Security.

4.8.1 Como fazer

Este capítulo contém algumas perguntas e problemas mais frequentes encontrados. Clique no título do capítulo para descobrir como solucionar o seu problema:

Como atualizar o ESET Mail Security

Como ativar o ESET Mail Security

Como agendar uma tarefa de rastreamento (a cada 24 horas)

Como remover um vírus do meu servidor

Como funcionam as exclusões automáticas

Se seu problema não estiver na lista de páginas de ajuda acima, tente pesquisar por palavra-chave ou frase, descrevendo seu problema e pesquisando nas Páginas de ajuda do ESET Mail Security.

Se não puder encontrar a solução para o seu problema/pergunta dentro das páginas de Ajuda, poderá tentar em nosso banco de dados de conhecimento online atualizado regularmente.

Se necessário, você pode contatar diretamente nosso centro de suporte técnico on-line com as suas perguntas ou problemas. O formulário de contato pode ser encontrado diretamente na guia Ajuda e Suporte do seu programa ESET.

4.8.1.1 Como atualizar o ESET Mail Security

A atualização do ESET Mail Security pode ser feita manual ou automaticamente. Para disparar a atualização, clique em **Atualizar banco de dados de assinatura de vírus**. Você encontrará isso na seção **Atualizar** do programa.

As configurações da instalação padrão criam uma tarefa de atualização automática que é executada a cada hora. Se precisar alterar o intervalo, vá para **Agenda** (para mais informações sobre a Agenda, clique aqui).

4.8.1.2 Como ativar o ESET Mail Security

Após a conclusão da instalação, você será solicitado a ativar o produto.

Há vários métodos para ativar seu produto. A disponibilidade de um cenário específico de ativação na janela de ativação pode variar conforme o país, assim como os meios de distribuição (CD/DVD, página da web da ESET etc.).

Para ativar sua cópia do ESET Mail Security diretamente do programa, clique no ícone da bandeja do sistema e selecione **Ativar licença do produto** no menu. Você também pode ativar seu produto do menu principal em **Ajuda e suporte** > **Ativar licença** ou **Status da proteção** > **Ativar licença do produto**.

Você pode usar qualquer um dos seguintes métodos para ativar o ESET Mail Security:

- **Chave de licença** - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usado para identificação do proprietário da licença e para ativação da licença.
- **Conta do Admin de segurança** - Uma conta criada no portal do ESET License Administrator com credenciais (endereço de email e senha). Esse método permite que você gerencie várias licenças de um local.
- Arquivo de **licença offline** - Um arquivo gerado automaticamente que será transferido para o produto da ESET para fornecer informações de licença. Seu arquivo de licença off-line é gerado do portal de licença e é usado em ambientes nos quais o aplicativo não pode se conectar à autoridade de licenciamento.

Clique em **Ativar mais tarde** com o ESET Remote Administrator se seu computador for um membro da rede gerenciada e seu administrador for realizar a ativação remota via ESET Remote Administrator. Você pode usar essa opção também caso queira ativar esse cliente posteriormente.

Clique em **Ajuda e suporte** > **Gerenciar licença** na janela do programa principal para gerenciar suas informações de licença a qualquer momento. Você verá o ID de licença pública para identificar seu produto pela ESET e para identificação de licença. Seu nome de usuário, sob o qual o computador está registrado com o sistema de licenciamento, é armazenado na seção **Sobre**, que pode ser vista clicando com o botão direito do mouse no ícone da bandeja do sistema.

OBSERVAÇÃO: ESET Remote Administrator é capaz de ativar computadores cliente em segundo plano usando licenças disponibilizadas pelo administrador.

4.8.1.3 Como criar uma nova tarefa na Agenda

Para criar uma nova tarefa em **Ferramentas** > **Agenda**, clique em **Adicionar tarefa** ou clique com o botão direito do mouse e selecione **Adicionar** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de relatório** - Os relatórios também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos relatórios para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um instantâneo do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, explicaremos a seguir como adicionar uma nova tarefa de atualização:

No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Insira o nome da tarefa no campo **Nome da tarefa** e clique em **Próximo**. Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Acionado por evento.** Selecione **Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Depois defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As opções disponíveis são:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem Tempo depois da última execução)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual é exibida. Clique em **Concluir** quando tiver concluído as alterações.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo. que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **Concluir** e a nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

4.8.1.4 Como agendar uma tarefa de rastreamento (a cada 24 horas)

Para agendar uma tarefa regular, vá para **ESET Mail Security** > **Ferramentas** > **Agenda**. A seguir, é possível localizar uma pequena guia sobre como agendar uma tarefa. Essa tarefa criará um rastreamento nas unidades locais a cada 24 horas.

Para agendar uma tarefa de rastreamento:

1. Clique em **Adicionar** na tela principal do módulo Agenda.
2. Selecione **Rastreamento sob demanda do computador** no menu suspenso.
3. Escolha um nome para a tarefa e selecione **Repetidamente**.
4. Escolha executar a tarefa a cada 24 horas (1440 minutos).
5. Selecione uma ação para executar se a execução da tarefa agendada falhar por algum motivo.
6. Revise o resumo da tarefa agendada e clique em **Fim**.
7. No menu suspenso **Alvos**, selecione Unidades locais.
8. Clique em **Concluir** para aplicar a tarefa.

4.8.1.5 Como remover um vírus do seu servidor

Se o seu computador estiver mostrando sintomas de uma infecção por código malicioso, como, por exemplo, estiver mais lento ou congelar com frequência, recomendamos que você faça o seguinte:

1. Na janela principal do ESET Mail Security, clique em **Rastrear o computador**.
2. Clique em **Rastreamento inteligente** para começar a rastrear o sistema.
3. Após a conclusão do rastreamento, revise o relatório com o número de arquivos verificados, infectados e limpos.
4. Se desejar rastrear apenas uma determinada parte do seu disco, selecione **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

4.8.2 Enviar solicitação de suporte

Para fornecer ajuda com a maior rapidez e precisão possíveis, a ESET solicita informações sobre a configuração do seu ESET Mail Security, informações detalhadas do sistema e processos em execução (relatório do ESET SysInspector) e dados do registro. A ESET usará estes dados apenas para fornecer assistência técnica ao cliente.

Quando enviar o formulário da web, seus dados de configuração do sistema serão enviados para a ESET. Selecione **Sempre enviar estas informações** se quiser lembrar desta ação para este processo. Para enviar o formulário sem mandar qualquer dado, clique em **Não enviar dados** e você pode entrar em contato com o Atendimento ao cliente ESET usando o formulário de suporte on-line.

Esta configuração também pode ser feita em **Configuração avançada** > **Ferramentas** > **Diagnóstico** > **Atendimento ao cliente**.

i **OBSERVAÇÃO**: Se você decidiu enviar dados do sistema é necessário preencher e enviar o formulário da web, caso contrário seu bilhete não será criado e os dados do seu sistema serão perdidos.

4.8.3 Limpador especializado ESET

O dispositivo de limpeza especializado ESET é uma ferramenta de remoção para infecções comuns de malware, como Conficker, Sirefef ou Necurs. Para obter mais informações, acesse este artigo do banco de conhecimento da ESET.

4.8.4 Sobre ESET Mail Security

Esta janela fornece detalhes sobre a versão instalada do ESET Mail Security e a lista de módulos do programa instalados. A parte superior da janela contém informações sobre o sistema operacional e os recursos do sistema.

eset MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

MONITORAMENTO
RELATÓRIOS
RASTREAR
QUARENTENA DE EMAIL
ATUALIZAR
CONFIGURAÇÃO
FERRAMENTAS
AJUDA E SUPORTE

ENJOY SAFER TECHNOLOGY™

Sobre

ESET Mail Security™, Versão 6.2.10009.1
A próxima geração da tecnologia NOD32.
Copyright © 1992-2015 ESET, spol. s r.o. Todos os direitos reservados.

Windows Server 2012 R2 Standard (64-bit), Versão 6.3.9600
Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2600 MHz), 12288 MB de RAM

Nome de usuário: FRANTO\administrator
Nome do computador: WIN-JLDLB8CEUR5

Componentes instalados: Copiar

Nome do componente	Versão	Data do build
Módulo de atualização: 1060 (20150617)	1060	6/17/2015
Módulo de rastreamento antivírus e antispyware: 1466 (20150813)	1466	8/13/2015
Módulo de heurística avançada: 1159 (20150820)	1159	8/20/2015
Módulo de suporte de arquivo: 1235 (20150728)	1235	7/28/2015
Módulo de limpeza: 1109 (20150519)	1109	5/19/2015
Suporte ao módulo Anti-Stealth: 1082 (20150803)	1082	8/3/2015

Aviso: Este programa é protegido por direitos autorais e tratados internacionais. A cópia ou a distribuição sem permissão expressa da ESET, spol. s r.o. por qualquer meio, em parte ou no todo, está estritamente proibida e resultará em processo judicial na extensão máxima permitida internacionalmente por essas leis.

Você pode copiar informações sobre os módulos (**Componentes instalados**) para a área de transferência clicando em **Copiar**. Isso pode ser útil durante a solução de problemas ou ao entrar em contato com o Suporte técnico.

4.8.5 Ativação do produto

Após a conclusão da instalação, você será solicitado a ativar o produto.

Há vários métodos para ativar seu produto. A disponibilidade de um cenário específico de ativação na janela de ativação pode variar conforme o país, assim como os meios de distribuição (CD/DVD, página da web da ESET etc.).

Para ativar sua cópia do ESET Mail Security diretamente do programa, clique no ícone da bandeja do sistema e selecione **Ativar licença do produto** no menu. Você também pode ativar seu produto do menu principal em **Ajuda e suporte** > **Ativar licença** ou **Status da proteção** > **Ativar licença do produto**.

Você pode usar qualquer um dos seguintes métodos para ativar o ESET Mail Security:

- **Chave de licença** - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usado para identificação do proprietário da licença e para ativação da licença.
- **Conta do Admin de segurança** - Uma conta criada no portal do ESET License Administrator com credenciais (endereço de email e senha). Esse método permite que você gerencie várias licenças de um local.
- Arquivo de **licença offline** - Um arquivo gerado automaticamente que será transferido para o produto da ESET para fornecer informações de licença. Seu arquivo de licença off-line é gerado do portal de licença e é usado em ambientes nos quais o aplicativo não pode se conectar à autoridade de licenciamento.

Clique em **Ativar mais tarde** com o ESET Remote Administrator se seu computador for um membro da rede gerenciada e seu administrador for realizar a ativação remota via ESET Remote Administrator. Você pode usar essa opção também caso queira ativar esse cliente posteriormente.

Clique em **Ajuda e suporte** > **Gerenciar licença** na janela do programa principal para gerenciar suas informações de licença a qualquer momento. Você verá o ID de licença pública para identificar seu produto pela ESET e para identificação de licença. Seu nome de usuário, sob o qual o computador está registrado com o sistema de licenciamento, é armazenado na seção **Sobre**, que pode ser vista clicando com o botão direito do mouse no ícone da bandeja do sistema .

OBSERVAÇÃO: ESET Remote Administrator é capaz de ativar computadores cliente em segundo plano usando licenças disponibilizadas pelo administrador.

4.8.5.1 Registro

Registre sua licença preenchendo os campos no formulário de registro e clicando em **Continuar**. Os campos marcados como necessários entre parênteses são obrigatórios. Essas informações serão usadas somente para questões envolvendo sua licença da ESET.

4.8.5.2 Ativação do administrador de segurança

A conta do administrador de segurança é uma conta criada no portal de licenças com seu **endereço de email** e **senha**, que é capaz de ver todas as autorizações de licença. Uma conta de administrador de segurança permite que você gerencie várias licenças. Se você não tiver uma conta de administrador de segurança, clique em **Criar conta** e você será redirecionado para a página da web do ESET License Administrator, onde poderá se registrar com suas credenciais.

Se você tiver esquecido sua senha, clique em **Esqueceu sua senha?** e será redirecionado para o portal ESET Business. Insira seu endereço de email e clique em **Enviar** para confirmar. Depois disso, você receberá uma mensagem com instruções para redefinir sua senha.

OBSERVAÇÃO: Para mais informações sobre usar o ESET License Administrator, consulte o Guia do Usuário do ESET License Administrator.

4.8.5.3 Falha na ativação

A ativação do ESET Mail Security não foi concluída com êxito. Certifique-se de que você tenha inserido a **Chave de licença** ou anexado uma **Licença off-line**. Se você tiver outra **Licença off-line**, insira-a novamente. Para verificar a chave de licença inserida, clique em **verificar novamente a chave de licença** ou em **comprar uma nova licença** e você será redirecionado à nossa página da web, onde poderá comprar uma nova licença.

4.8.5.4 Licenças

Se você escolher a opção de ativação do Administrador de segurança, será solicitado que selecione uma licença associada à sua conta que será usada para o ESET Mail Security. Clique em **Ativar** para continuar.

4.8.5.5 Progresso da ativação

O ESET Mail Security está sendo ativado, aguarde. Isso pode levar alguns minutos.

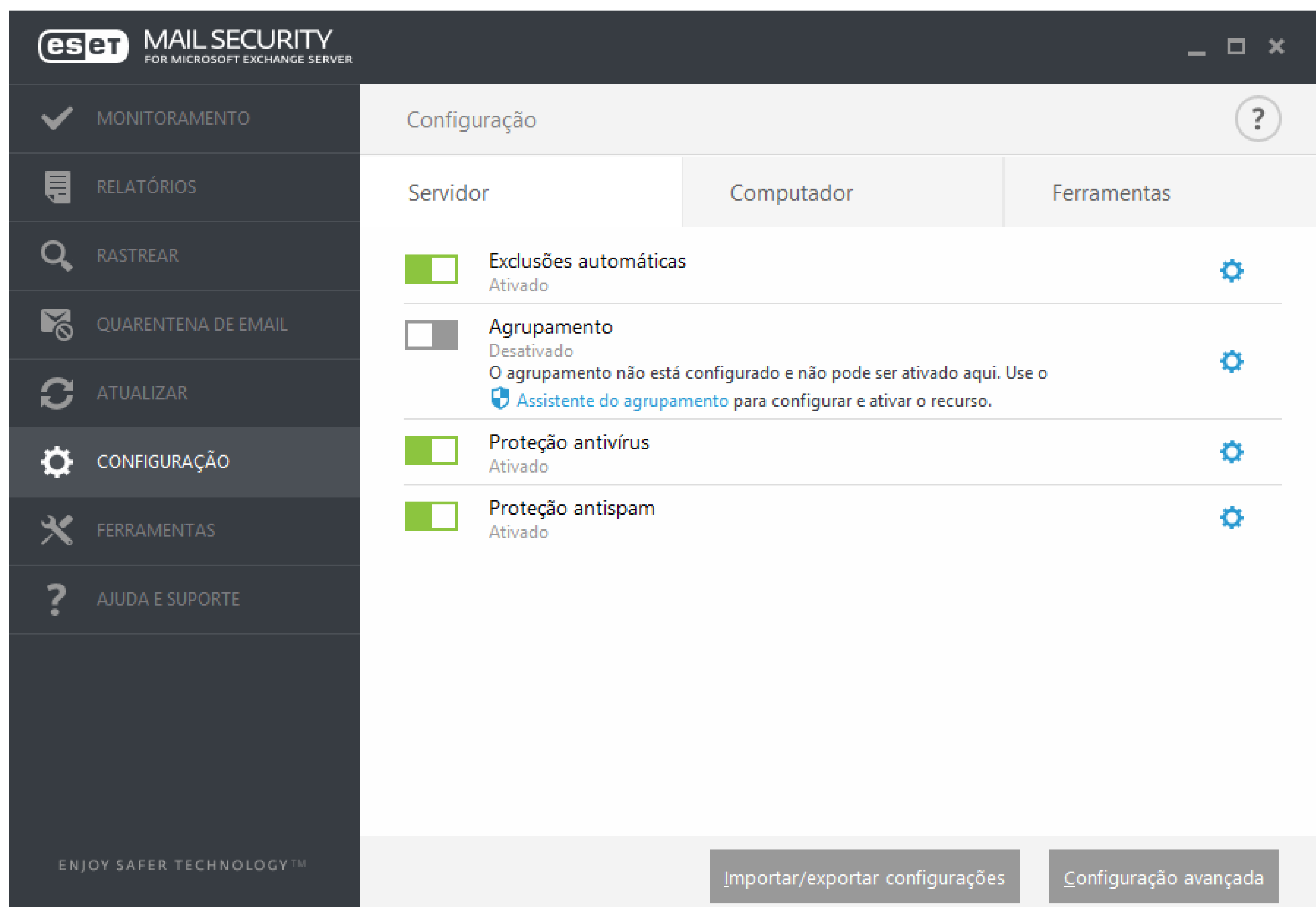
4.8.5.6 Ativação bem sucedida

A ativação foi concluída com êxito e o ESET Mail Security agora está ativado. A partir de agora, o ESET Mail Security receberá atualizações regulares para identificar as ameaças mais recentes e manter seu computador protegido. Clique em **Concluído** para concluir a ativação do produto.

5. Trabalhando com o ESET Mail Security

O menu de **Configuração** contém as seguintes seções entre as quais você pode alternar usando guias:

- Servidor
- Computador
- Ferramentas



Para desativar os módulos individuais temporariamente, clique na opção verde ao lado do módulo desejado. Observe que essa ação pode diminuir o nível de proteção do seu computador.
Para reativar a proteção do componente de segurança desativado, clique na opção vermelha para retornar um componente a seu estado ativado.
Para acessar configurações detalhadas de um componente de segurança específico, clique no ícone de engrenagem .

Clique em **Configuração avançada** ou pressione **F5** para acessar configurações e opções adicionais de componentes.

Existem opções adicionais na parte inferior da janela de configuração. Use **Configurações importar/exportar** para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar os parâmetros atuais em um arquivo de configuração. Para obter informações mais detalhadas, consulte Importar/Exportar configurações.

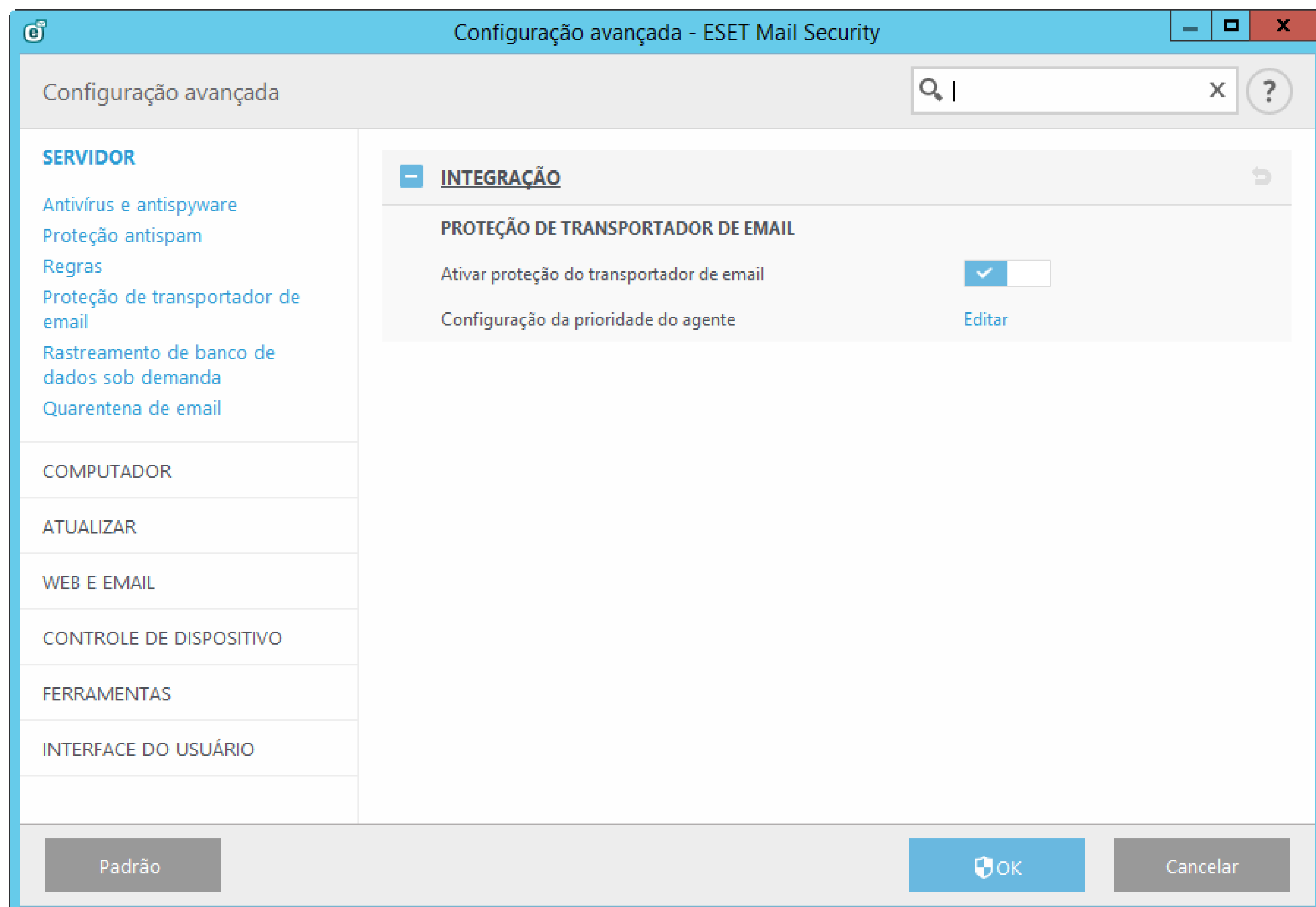
5.1 Servidor

o ESET Mail Security fornece proteção significativa para o Microsoft Exchange Server usando os recursos a seguir:

- Antivírus e antispyware
- Proteção antispam
- Permissões
- Proteção de transportador de email (Exchange Server 2007, 2010, 2013)
- Proteção do banco de dados da caixa de entrada (Exchange Server 2003, 2007, 2010)
- Rastreamento de banco de dados sob demanda (Exchange Server 2007, 2010, 2013)
- Quarentena (Configurações de tipo de quarentena de email)

A seção de Configuração avançada permite ativar ou desativar a integração da Proteção do banco de dados da caixa de entrada e Proteção de transportador de email assim como editar a Prioridade do agente.

OBSERVAÇÃO: Se estiver executando o Microsoft Exchange Server 2007 ou 2010 é possível escolher entre o rastreamento de Proteção do banco de dados da caixa de entrada e Banco de dados sob demanda. Porém, apenas um tipo de proteção entre esses dois pode estar ativo por vez. Se decidir usar o rastreamento de banco de dados sob demanda, será preciso desativar a integração da Proteção do banco de dados da caixa de entrada. Caso contrário o Rastreamento de banco de dados sob demanda não estará disponível.



5.1.1 Configuração da prioridade do agente

No menu **Configuração da prioridade do agente**, é possível configurar a prioridade na qual os Agentes ESET Mail Security são ativados depois do Microsoft Exchange Server ser iniciado. O valor numérico define a prioridade. Quanto menor for o número, maior será a prioridade. Isto se aplica ao Microsoft Exchange 2003.

Clique no botão **Editar** para entrar na configuração da prioridade do Agente, onde é possível configurar a prioridade na qual os Agentes ESET Mail Security são ativados depois do início do Microsoft Exchange Server.

- **Modificar** - define manualmente o número para alterar a prioridade do Agente selecionado.
- **Mover para cima** - aumenta a prioridade do Agente selecionado ao movê-lo para cima na lista de Agentes.
- **Mover para baixo** - diminui a prioridade do Agente selecionado ao movê-lo para baixo na lista de Agentes.

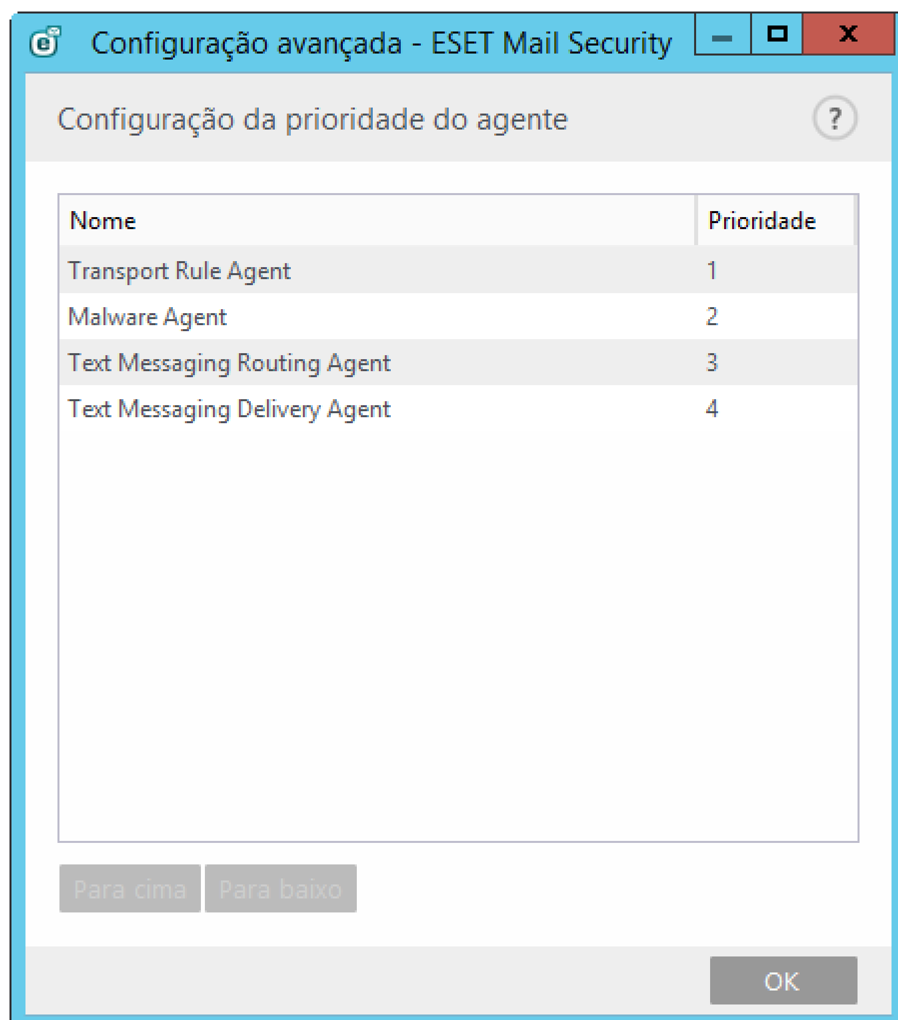
Com o Microsoft Exchange Server 2003, é possível especificar a prioridade do Agente independentemente, usando guias para EOD (fim de dados) e RCPT (destinatário).

5.1.1.1 Modificar prioridade

Se estiver executando o Microsoft Exchange Server 2003, é possível definir manualmente o número para alterar a **Prioridade do agente de transporte**. Modifique o número no campo de texto ou use as setas para cima ou para baixo para alterar a prioridade. Quanto menor for o número, maior será a prioridade.

5.1.2 Configuração da prioridade do agente

No menu **Configuração da prioridade do agente**, é possível configurar a prioridade na qual os Agentes ESET Mail Security são ativados depois do Microsoft Exchange Server ser iniciado. Isto se aplica ao Microsoft Exchange 2007 e posterior.



- **Mover para cima** - aumenta a prioridade do Agente selecionado ao movê-lo para cima na lista de Agentes.

- **Mover para baixo** - diminui a prioridade do Agente selecionado ao movê-lo para baixo na lista de Agentes.

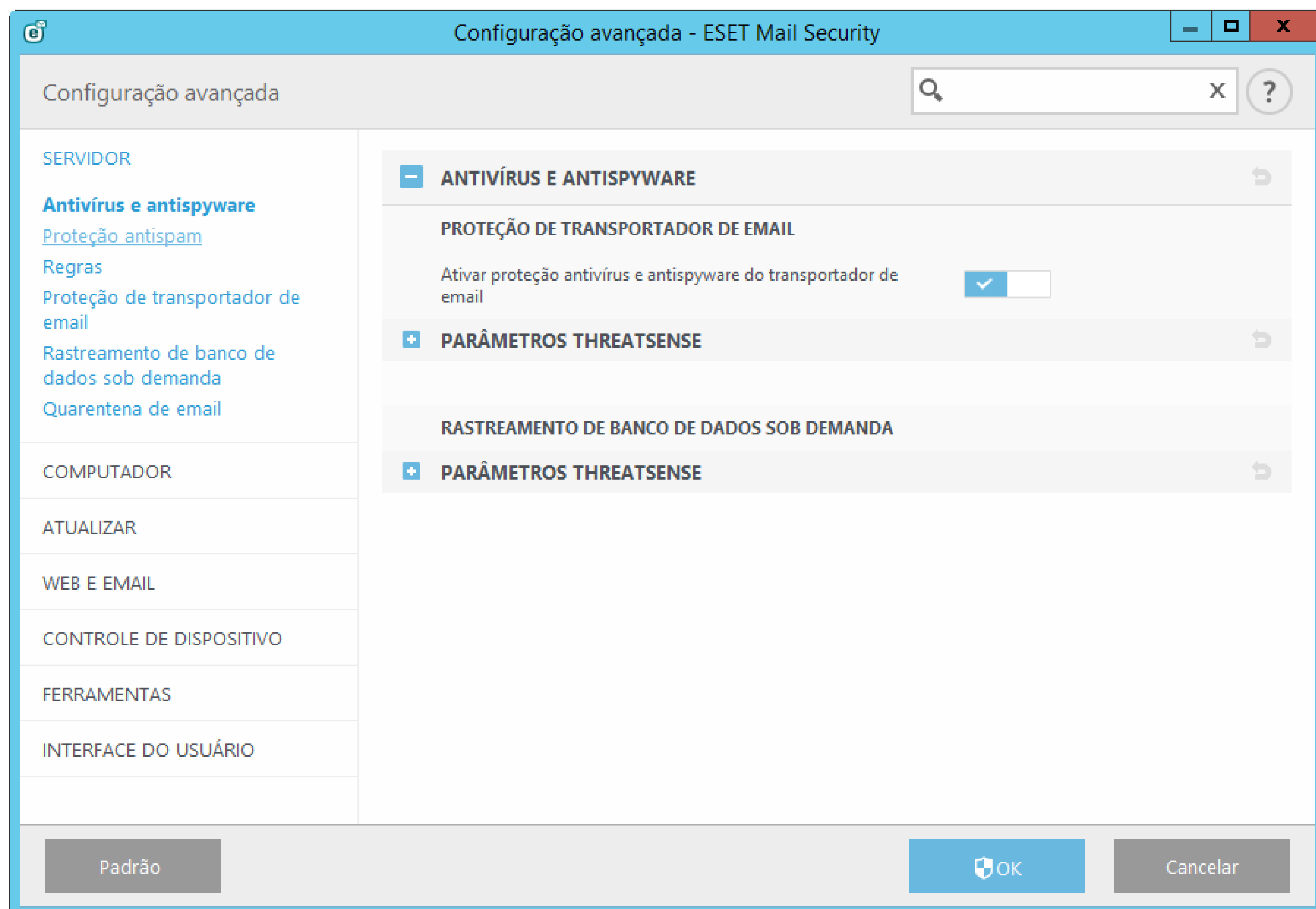
5.1.3 Antivírus e antispyware

Nesta seção, você pode configurar opções de **Antivírus e antispyware** para seu servidor de email.

Importante: A Proteção de transportador de email é fornecida pelo agente de transporte e só está disponível para Microsoft Exchange Server 2007 ou mais recente, mas seu Exchange Server deve ter a função Servidor Edge Transport ou Servidor Hub Transport. Isto também é aplicável em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que tenha a função Edge ou Hub Transport).

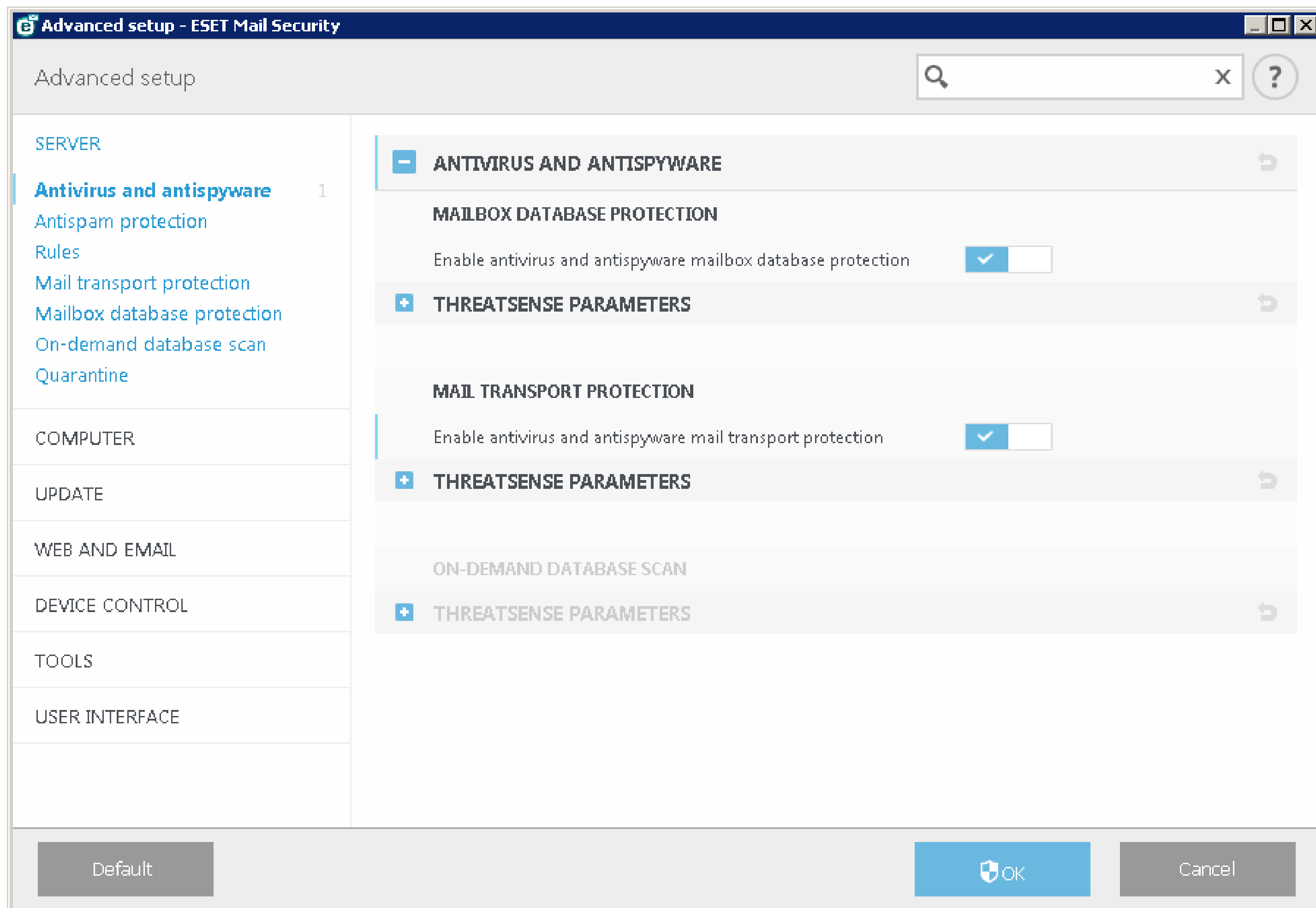
Proteção de transportador de email:

Se **Ativar proteção antivírus e antispyware do transportador de email** for desativado, o plug-in do ESET Mail Security para Exchange Server não será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus na camada de transporte. As mensagens ainda serão rastreadas em busca de vírus e spam na camada do banco de dados e as regras existentes serão aplicadas.



Proteção do banco de dados da caixa de entrada:

Se **Ativar proteção antivírus e antispyware do banco de dados da caixa de entrada** for desativado, o plug-in do ESET Mail Security para Exchange Server não será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus na camada de banco de dados. As mensagens ainda serão rastreadas em busca de vírus e spam na camada do banco de dados e as regras existentes serão aplicadas.



5.1.4 Proteção antispam

Por padrão, a proteção antispam para seu servidor de email está ativada. Para desligar, clique no botão ao lado de **Ativar proteção antispam**.

Ativar **Usar listas de permissão do Exchange Server para ignorar automaticamente a proteção antispam** permite que o ESET Mail Security use "lista de permissões" específicas do Exchange. Quando ativada, o seguinte é levado em consideração:

- O endereço IP do servidor está na lista de IP permitido do Exchange Server
- O destinatário da mensagem tem o sinalizador Ignorar antispam definido como ativo em sua caixa de correio
- O destinatário da mensagem tem o endereço do remetente na Lista de remetentes seguros (certifique-se de que você tenha configurado a Sincronização da lista de remetentes seguros em seu ambiente do Exchange Server, incluindo Agregação da lista segura)

Se qualquer um dos acima se aplicar a uma mensagem recebida, a verificação antispam será desviada para essa mensagem, a mensagem não será avaliada quanto a SPAM e será entregue na caixa de correio do destinatário.

A opção **Aceitar sinalizador de ignorar antispam definido na sessão SMTP** é útil quando você tem sessões SMTP entre servidores Exchange com a configuração de ignorar antispam. Por exemplo, quando você tiver um servidor de Edge e um servidor de Hub, não há necessidade de rastrear o tráfego entre os dois servidores. A opção **Aceitar sinalizador de ignorar antispam definido na sessão SMTP** está ativada por padrão, mas só se aplica quando o sinalizador de ignorar antispam é configurado para a sessão SMTP no seu Exchange Server. Se você desativar **Aceitar sinalização de ignorar antispam definida em sessão SMTP**, o ESET Mail Security vai rastrear a sessão SMTP em busca de spam independente da configuração de desvio de antispam no seu Exchange Sever.

OBSERVAÇÃO: É necessário que o banco de dados Antispam seja atualizado regularmente para que o módulo Antispam forneça a melhor proteção possível. Para permitir atualizações regulares no banco de dados Antispam, certifique-se de que o ESET Mail Security tem acesso ao endereço IP correto nas portas necessárias. Para obter mais informações sobre quais IPs e portas permitir em seu firewall de terceiros, leia nosso artigo da base de

conhecimento.

5.1.4.1 Filtragem e verificação

É possível configurar listas **permitidas**, **bloqueadas** e **ignoradas** ao especificar critérios, como endereço IP ou intervalo, nome de domínio, etc. Para adicionar, modificar ou remover critérios, clique em **Editar** para a lista que deseja gerenciar.

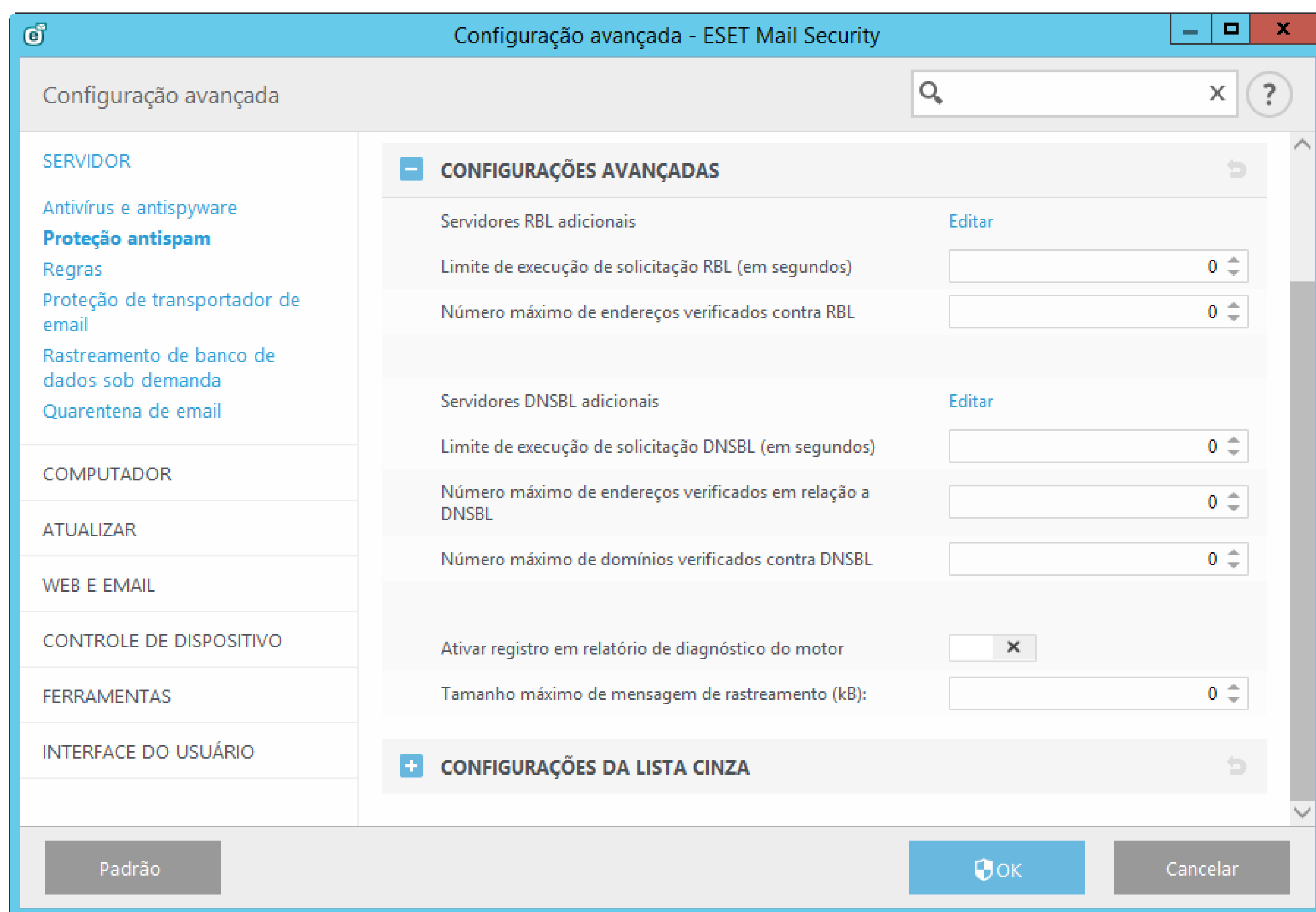
- **Lista de IP aprovada**
- **Lista de IP bloqueada**
- **Lista de IP ignorada**
- **Lista de Domínio do Corpo bloqueado**
- **Lista de Domínio do Corpo ignorado**
- **Lista de corpo de IP bloqueado**
- **Lista de corpo de IP ignorado**
- **Lista de remetentes aprovados**
- **Lista de remetentes bloqueados**
- **Domínio aprovado para lista de IP**
- **Domínio bloqueado para lista de IP**
- **Domínio ignorado para lista de IP**
- **Lista de conjuntos de caracteres bloqueados**
- **Lista de países bloqueados**

5.1.4.2 Configurações avançadas

Essas configurações permitem que as mensagens sejam verificadas por servidores externos (**RBL** - Lista de bloqueios em tempo real, **DNSBL** - Lista de bloqueio de DNS) de acordo com os critérios definidos.

Limite de execução de solicitação da RBL (em segundos): - Esta opção permite definir um tempo máximo para consultas RBL. As respostas da RBL são usadas somente a partir desses servidores da RBL que respondem em tempo hábil. Se o valor for "0", nenhum limite de tempo será forçado.

Número máximo de endereços verificados em relação à RBL: - Essa opção permite limitar quantos endereços IP são consultados em relação ao servidor da RBL. Observe que o número total de consultas da RBL será o número de endereços IP nos cabeçalhos Recebidos: (até um máximo de endereços IP de verificação máxima de RBL) multiplicado pelo número de servidores da RBL especificados na lista da RBL. Se o valor for definido como "0", o número ilimitado de cabeçalhos recebidos será verificado. Observe que IPs na lista de IP ignorado não contam em relação ao limite de endereços IP da RBL.



Limite de execução de solicitação da DNSBL (em segundos): - Permite configurar um limite de tempo máximo para a conclusão de todas as consultas da DNSBL.

Número máximo de endereços verificados em relação a DNSBL: - Permite limitar quantos endereços IP são consultados em relação ao servidor da Lista de bloqueios de DNS.

Número máximo de domínios verificados em relação à DNSBL: - Permite limitar quantos domínios são consultados em relação ao servidor da Lista de bloqueios de RBL.

Serviço RBL: - Especifica uma lista de servidores da RBL (Realtime Blackhole List, Lista de bloqueios em tempo real) para consulta ao analisar mensagens. Consulte a seção da RBL neste documento para obter mais informações.

Serviço DNSBL: - Especifica uma lista de servidores da Lista de bloqueio de DNS (DNSBL) para consulta com domínios e IPs extraídos do corpo da mensagem.

Ativar registro em relatório de diagnóstico do motor - Escreve informações detalhadas sobre o mecanismo antispam nos relatórios para fins de diagnóstico.

Tamanho máximo de mensagem de rastreamento (kB):- Limita o rastreamento Antispam para mensagens maiores do que o valor especificado. Essas mensagens não serão rastreadas pelo mecanismo antispam.

5.1.4.3 Configurações da lista cinza

A função **Ativar lista cinza** ativa um recurso que protege os usuários contra spam usando a seguinte técnica: O agente de transporte enviará o valor de retorno SMTP "rejeitar temporariamente" (o padrão é 451/4.7.1) para qualquer email recebido que não seja de um remetente reconhecido. Um servidor legítimo tentará reenviar a mensagem após um atraso. Os servidores de spam normalmente não tentam reenviar a mensagem, pois costumam passar por milhares de endereços de email e não perdem tempo com reenvio. A Lista cinza é uma camada adicional de proteção antispam e não tem efeito sobre as capacidades de avaliação de spam do módulo antispam.

Ao avaliar a origem da mensagem, o método de Lista cinza leva em conta a **Lista de IP aprovada**, a **Lista de IP ignorada**, **Remetentes seguros**e a **Lista de IP aprovada** no servidor do Exchange, assim como as configurações AntispamBypass para a caixa de entrada do destinatário. Os emails desses endereços IP/listas de remetentes ou emails entregues a uma caixa de correio que tem a opção AntispamBypass ativada serão ignorados pelo método de detecção de lista cinza.

Usar apenas a parte de domínio do endereço do remetente - ignora o nome do destinatário no endereço de email, apenas o domínio é levado em conta.

Limite de tempo para recusa da conexão inicial (min.) – quando uma mensagem é entregue pela primeira vez e é negada temporariamente, esse parâmetro define o período de tempo durante o qual a mensagem será sempre negada (medido a partir da primeira vez que é negada). Após o período definido ter decorrido, a mensagem será recebida com êxito. O valor mínimo que pode ser inserido é de 1 minuto.

Tempo de expiração das conexões não verificadas (horas) – esse parâmetro define o intervalo de tempo mínimo no qual os dados do trio serão armazenados. Um servidor válido deve reenviar uma mensagem desejada antes que esse período expire. Esse valor deve ser superior ao valor do **Limite de tempo para recusa da conexão inicial**.

Tempo de expiração das conexões verificadas (dias) – o número mínimo de dias em que as informações do trio serão armazenadas, durante o qual os emails de um remetente específico serão recebidos sem atraso. Esse valor deve ser superior ao valor de **Tempo de expiração das conexões não verificadas**.

Resposta SMTP (para conexões negadas temporariamente) - é possível especificar um **Código de resposta**, **Código do status** e **Mensagem de resposta**, que definem a resposta de negação temporária de SMTP enviada para o servidor SMTP se uma mensagem for recusada.

Exemplo de uma mensagem de resposta de rejeição SMTP:

Código de resposta	Código do status	Mensagem de resposta
451	4.7.1	Ação solicitada anulada: erro local no processamento

AVISO: Sintaxe incorreta nos códigos de resposta SMTP pode causar mau funcionamento da proteção de lista cinza. Como resultado, as mensagens de spam podem ser entregues aos clientes ou as mensagens podem não ser entregues.

OBSERVAÇÃO: Também é possível usar variáveis do sistema ao definir a resposta de rejeição SMTP.

5.1.5 Regras

As **Regras** permitem que os administradores definam manualmente as condições de filtragem de email e as ações a serem tomadas com os emails filtrados.

Existem três grupos de regras separados. As regras disponíveis no seu sistema dependem de qual versão do Microsoft Exchange Server está instalada no servidor com o ESET Mail Security:

- Proteção do banco de dados da caixa de entrada - Este tipo de proteção só está disponível para o Microsoft Exchange Server 2010, 2007 e 2003 operando na função Servidor Mailbox (Microsoft Exchange 2010 e 2007) ou Servidor Back-End (Microsoft Exchange 2003). Este tipo de rastreamento pode ser realizado em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que inclua a função de Mailbox ou Back-end).

- Proteção de transportador de email - Esta proteção é fornecida pelo agente de transporte e só está disponível para Microsoft Exchange Server 2007 ou mais recente operando na função de Servidor Edge Transport ou Servidor Hub Transport. Este tipo de rastreamento pode ser realizado em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que tenha uma das funções de servidor mencionadas).

- Rastreamento de banco de dados sob demanda - permite executar ou agendar um rastreamento do banco de dados de caixa de entrada Exchange. Este recurso só está disponível para Microsoft Exchange Server 2007 ou mais recente operando na função Servidor Mailbox ou Transporte de Hub. Isto também é aplicável em uma instalação de servidor única com várias funções do Exchange Server em um computador (desde que tenha uma das funções de servidor mencionadas). Veja funções do Exchange Server 2013 para detalhes específicos sobre funções no Exchange 2013.

5.1.5.1 Lista de regras

Uma regra é composta por **condições** e **ações**. Assim que todas as condições forem cumpridas para uma mensagem de email, as ações serão realizadas naquela mensagem de email. Em outras palavras, as regras são aplicadas de acordo com um conjunto de condições combinadas. Se existirem várias condições para a regra, elas serão combinadas usando o operador lógico AND e a regra só será aplicada se as condições forem cumpridas.

A janela da lista de **Regras** exibe as regras existentes. Regras são classificadas em três níveis e são avaliadas na seguinte ordem:

- **Regras de filtragem (1)**
- **Regras de processamento de anexo (2)**
- **Regras de processamento de resultado (3)**

Regras com o mesmo nível são avaliadas na mesma ordem em que são exibidas na janela de Regras. Você só pode alterar a ordem das regras para as regras do mesmo nível. Por exemplo, quando você tem várias regras de filtragem, você pode alterar a ordem na qual elas são aplicadas. Você não pode alterar a ordem colocando regras de Processamento de anexos antes das regras de Filtragem, os botões Para cima/Para baixo não estarão disponíveis. Em outras palavras, você não pode misturar regras de níveis diferentes.

A coluna Acessor exibe o número de vezes que a regra foi aplicada com êxito. Desmarcar uma caixa de seleção (na esquerda do nome de cada regra) desativa a regra correspondente até que você marque a caixa de seleção novamente.

- **Adicionar...** - adiciona uma nova regra
- **Editar...** - modifica uma regra existente
- **Remover** – remove a regra selecionada
- **Mover para cima** - move a regra selecionado para cima na lista
- **Mover para baixo** - move a regra selecionada para baixo na lista
- **Redefinir** - redefine o contador para a regra selecionada (a coluna Acessos)

i **OBSERVAÇÃO**: Se uma nova regra for adicionada ou uma regra existente foi modificada, um novo rastreamento das mensagens começará automaticamente a usar as regras novas/modificadas.

As regras são verificadas em relação à mensagem quando ela é processada pelo agente de transporte (TA) ou pela VSAPI. Quando o TA e a VSAPI estão ativados e a mensagem corresponde às condições da regra, o contador de regras pode aumentar em 2 ou mais. Isto acontece porque o VSAPI acessa o corpo e os anexos de uma mensagem separadamente, então as regras são aplicadas para cada parte individualmente. As regras também são aplicadas durante o rastreamento em segundo plano (por exemplo, quando o ESET Mail Security executa uma verificação da caixa de entrada depois do download de um novo banco de dados de assinatura de vírus), o que pode aumentar o contador da regra.

5.1.5.1.1 Assistente de regra

Você pode definir **Condições** e **Ações** usando o assistente de **Regra**. Defina primeiro as Condições, depois as Ações. Clique em **Adicionar** e uma janela de Condição de regra aparece, onde você pode selecionar o tipo de condição, operação e valor. A partir daí, você pode adicionar uma Ação de regra. Assim que as condições e ações são definidas, digite um **Nome** para a regra (algo pelo qual você vai reconhecer a regra), esse nome será exibido na Lista de regras. Se quiser preparar regras mas planeja usá-las mais tarde, você pode clicar no botão ao lado de **Ativo** para desativar a regra. Para ativar a regra, marque a caixa de seleção ao lado da regra que deseja ativar na Lista de regras.

Algumas **Condições** e **Ações** diferem para regras específicas para a **Proteção de transportador de email**, **Proteção do banco de dados da caixa de entrada** e **Rastreamento de banco de dados sob demanda**. Isso acontece porque cada um desses tipos de proteção usa uma abordagem um pouco diferente ao processar mensagens, especialmente a **Proteção de transportador de email**.

Configuração avançada - ESET Mail Security
Regra
Ativo
Nome

Tipo de condição	Operation	Parâmetros

Adicionar Editar Remover

Tipo de ação	Parâmetro

Adicionar Editar Remover

OK Cancelar

5.1.5.1.1.1 Condição de regra

Este assistente permite que você adicione condições para uma regra. Selecione **Tipo** > **Operação** na lista suspensa (a lista de operações muda dependendo do tipo de regra que você escolheu) e selecione **Parâmetros**. Os campos de Parâmetros vão mudar dependendo do tipo de regra e operação.

Por exemplo, escolha o **Tamanho do anexo** > **Maior do que** e em **Parâmetro** especifique 10 MB. Usando essas configurações, qualquer mensagem que contém um anexo maior do que 10 MB será processada usando a ação de regra que você especificou. Por isso, você deve especificar qual ação é realizada quando uma determinada regra é acionada, se isso não tiver sido feito ao definir parâmetros para a regra.

i **OBSERVAÇÃO:**É possível adicionar várias condições para uma regra. Ao adicionar condições múltiplas, condições que anulam umas às outras não serão exibidas.

As **Condições** a seguir estão disponíveis para **Proteção de transporte de email** (algumas opções podem não aparecer, dependendo das suas condições selecionadas anteriormente):

- **Assunto** - aplicável a mensagens que contêm ou não contêm uma string específica (ou uma expressão regular) no assunto.
- **Remetente** - aplicável a mensagens enviadas por um remetente específico
- **Destinatário** - aplicável a mensagens enviadas para um destinatário específico
- **Nome do anexo** - aplicável a mensagens que contenham anexos com um nome específico
- **Tamanho do anexo** - aplicável a mensagens com um anexo que não atende a um tamanho especificado, está dentro de um intervalo de tamanho especificado, ou ultrapassa um tamanho especificado
- **Tipo de anexo** - aplicável a mensagens com um tipo específico de arquivo anexado. Tipos de arquivos são categorizados em grupos para facilitar a seleção, é possível selecionar vários tipos de arquivos ou categorias inteiras
- **Tamanho da mensagem** - aplicável a mensagens com anexos que não atendem a um tamanho especificado, estão dentro de um intervalo de tamanho especificado, ou ultrapassam um tamanho especificado
- **Resultado do rastreamento antispam** - aplicável a mensagens sinalizadas ou não sinalizadas como Ham ou Spam
- **Resultado do rastreamento antivírus** - aplicável a mensagens sinalizadas como maliciosas ou não maliciosas
- **Mensagem interna** - aplicável dependendo da mensagem ser interna ou não
- **Hora em que foi recebido** - aplicável a mensagens recebidas antes ou depois de uma data específica, ou durante um período específico
- **Cabeçalhos de mensagens** - aplicável a mensagens com dados específico presentes no cabeçalho da mensagem
- **Contém arquivo protegido por senha** - aplicável a mensagens com anexos de arquivos que são protegidos por senha
- **Contém arquivo danificado** - aplicável a mensagens com anexos de arquivos que estão danificados (provavelmente impossíveis de abrir)
- **Endereço IP do remetente** - aplicável a mensagens enviadas de um endereço IP específico
- **Domínio do remetente** - aplicável a mensagens de um remetente com um domínio específico em seus endereços de email

- **Unidades organizacionais do remetente** - aplicável a mensagens enviadas para um destinatário de uma unidade organizacional específica

Lista de Condições disponíveis para Proteção do banco de dados da caixa de entrada e Rastreamento de banco de dados sob demanda (algumas das opções podem não aparecer, isso depende de determinadas condições):

- **Assunto** - aplicável a mensagens que contêm ou não contêm uma string específica (ou uma expressão regular) no assunto.
- **Remetente** - aplicável a mensagens enviadas por um remetente específico
- **Destinatário** - aplicável a mensagens enviadas para um destinatário específico
- **Caixa de entrada** - aplicável a mensagens localizadas em uma caixa de entrada específica
- **Nome do anexo** - aplicável a mensagens que contenham anexos com um nome específico
- **Tamanho do anexo** - aplicável a mensagens com um anexo que não atende a um tamanho especificado, está dentro de um intervalo de tamanho especificado, ou ultrapassa um tamanho especificado
- **Tipo de anexo** - aplicável a mensagens com um tipo específico de arquivo anexado. Tipos de arquivos são categorizados em grupos para facilitar a seleção, é possível selecionar vários tipos de arquivos ou categorias inteiras
- **Resultado do rastreamento antivírus** - **Resultado do rastreamento antivírus** - aplicável a mensagens sinalizadas como maliciosas ou não maliciosas
- **Hora em que foi recebido** - aplicável a mensagens recebidas antes ou depois de uma data específica, ou durante um período específico
- **Cabeçalhos de mensagens** - aplicável a mensagens com dados específico presentes no cabeçalho da mensagem
- **Contém arquivo protegido por senha** - aplicável a mensagens com anexos de arquivos que são protegidos por senha
- **Contém arquivo danificado** - aplicável a mensagens com anexos de arquivos que estão danificados (provavelmente impossíveis de abrir)
- **Endereço IP do remetente** - aplicável a mensagens enviadas de um endereço IP específico
- **Domínio do remetente** - aplicável a mensagens de um remetente com um domínio específico em seus endereços de email

5.1.5.1.1.2 Ação de regra

Você pode adicionar ações que serão realizadas com mensagens e/ou anexos que correspondem a condições da regra.

i **OBSERVAÇÃO:**É possível adicionar várias condições para uma regra. Ao adicionar condições múltiplas, condições que anulam umas às outras não serão exibidas.

A lista de **Ações** disponíveis para **Proteção de transporte de email** (algumas opções podem não aparecer, dependendo das suas condições selecionadas):

- **Mensagem em quarentena** - a mensagem não será entregue ao destinatário e será movida para a quarentena de email
- **Excluir anexo -** exclui um anexo de mensagem, a mensagem será entregue ao destinatário sem o anexo
- **Rejeitar mensagem** - a mensagem não será entregue e um NDR (Relatório de não entrega) será enviado ao remetente
- **Ignorar mensagem silenciosamente** - exclui uma mensagem sem enviar uma NDR

- **Definir SCL valor** - altera ou define um valor SCL específico
- **Enviar relatório** - envia um relatório
- **Pular rastreamento Antispam** - a mensagem será rastreada pelo mecanismo antispam
- **Pular rastreamento Antivírus** - a mensagem será rastreada pelo mecanismo antivírus
- **Avaliar outras regras** - permite a avaliação de outras regras, permitindo ao usuário definir vários conjuntos de condições e várias ações a serem tomadas, de acordo com as condições
- **Relatório** – salva as informações sobre a regra aplicada no relatório do programa
- **Adicionar cabeçalho arquivado** - adiciona uma string personalizada em um cabeçalho de mensagem

A lista de **Ações** disponíveis para **Proteção do banco de dados da caixa de entrada** e **Rastreamento de banco de dados sob demanda** (algumas das opções podem não aparecer, isso depende de determinadas condições):

- **Excluir anexo -** exclui um anexo de mensagem, a mensagem será entregue ao destinatário sem o anexo
- **Anexo em quarentena** - coloca anexo de email para na quarentena de email, o email será entregue ao destinatário sem o anexo
- **Substituir anexo com informações sobre a ação** - remove um anexo e adiciona informações sobre as medidas tomadas para o anexo no corpo do email
- **Excluir mensagem** - exclui a mensagem
- **Enviar relatório** - envia um relatório
- **Pular rastreamento Antivírus** - a mensagem será rastreada pelo mecanismo antivírus
- **Avaliar outras regras** - permite a avaliação de outras regras, permitindo ao usuário definir vários conjuntos de condições e várias ações a serem tomadas, de acordo com as condições
- **Relatório** – salva as informações sobre a regra aplicada no relatório do programa
- **Mover mensagem para o lixo** (disponível apenas para **Rastreamento de banco de dados sob demanda**) - coloca uma mensagem de email na pasta de lixo do lado do cliente de email

5.1.6 Proteção do banco de dados da caixa de entrada

Os sistemas a seguir tem **Proteção do banco de dados da caixa de entrada** disponível em **Configurações avançadas** > **Servidor**:

- Microsoft Exchange Server 2003 (função de servidor Back-End)
- Microsoft Exchange Server 2003 (instalação de servidor única com várias funções)
- Microsoft Exchange Server 2007 (função de servidor Mailbox)
- Microsoft Exchange Server 2007 (instalação de servidor única com várias funções)
- Microsoft Exchange Server 2010 (função de servidor Mailbox)
- Microsoft Exchange Server 2010 (instalação de servidor única com várias funções)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

OBSERVAÇÃO: Proteção do banco de dados da caixa de entrada não está disponível para Microsoft Exchange Server 2013.

Se **Ativar proteção antivírus e antispyware VSAPI 2.6** for desmarcado, o plug-in do ESET Mail Security para Exchange Server não será descarregado do processo do Microsoft Exchange Server. Ele só passará pelas mensagens sem o rastreamento quanto a vírus. Entretanto, as mensagens ainda serão rastreadas quanto a spam e as regras serão aplicadas.

Se **Rastreamento proativo** estiver ativado, as novas mensagens recebidas serão rastreadas na mesma ordem em que foram recebidas. Se essa opção estiver ativada e um usuário abrir uma mensagem que ainda não tenha sido rastreada, essa mensagem será rastreada antes das outras mensagens na fila.

Rastreamento em segundo plano permite que o rastreamento de todas as mensagens seja executado em segundo plano (o rastreamento é executado na caixa de entrada e nas pastas públicas, por exemplo no banco de dados do Exchange). O Microsoft Exchange Server decide se um rastreamento em segundo plano será executado ou não com base em vários fatores, como a carga do sistema atual, o número de usuários ativos, etc. O Microsoft Exchange Server mantém um relatório das mensagens rastreadas e da versão do banco de dados de assinatura de vírus usado. Se você estiver abrindo uma mensagem que não tenha sido rastreada pelo banco de dados de assinatura de vírus mais recente, o Microsoft Exchange Server enviará a mensagem para o ESET Mail Security para ela ser rastreada antes da abertura da mensagem em seu cliente de email. É possível optar por **Rastrear somente mensagens com anexos** e filtrar de acordo com a hora recebida com as seguintes opções de **Nível de rastreamento**:

- **Todas as mensagens**
- **Mensagens recebidas no último ano**
- **Mensagens recebidas nos últimos 6 meses**
- **Mensagens recebidas nos últimos 3 meses**
- **Mensagens recebidas no último mês**
- **Mensagens recebidas na última semana**

Como o rastreamento em segundo plano pode afetar a carga do sistema (o rastreamento é realizado depois de cada atualização do banco de dados de assinatura de vírus), recomendamos agendar o rastreamento para ser executado fora do horário de trabalho. O rastreamento em segundo plano agendado pode ser configurado por meio de uma tarefa especial na Agenda/Planejamento. Ao agendar uma tarefa de rastreamento em segundo plano, é possível definir a hora de início, o número de repetições e outros parâmetros disponíveis na Agenda/Planejamento. Depois que a tarefa tiver sido agendada, ela será exibida na lista de tarefas agendadas e será possível modificar seus parâmetros, excluí-la ou desativá-la temporariamente.

A ativação da opção **Rastrear corpo das mensagens em RTF** ativa o rastreamento do corpo das mensagens em RTF. O corpo das mensagem em RTF pode conter vírus de macro.

i **OBSERVAÇÃO:** O corpo de email com texto simples não é rastreado pela VSAPI.

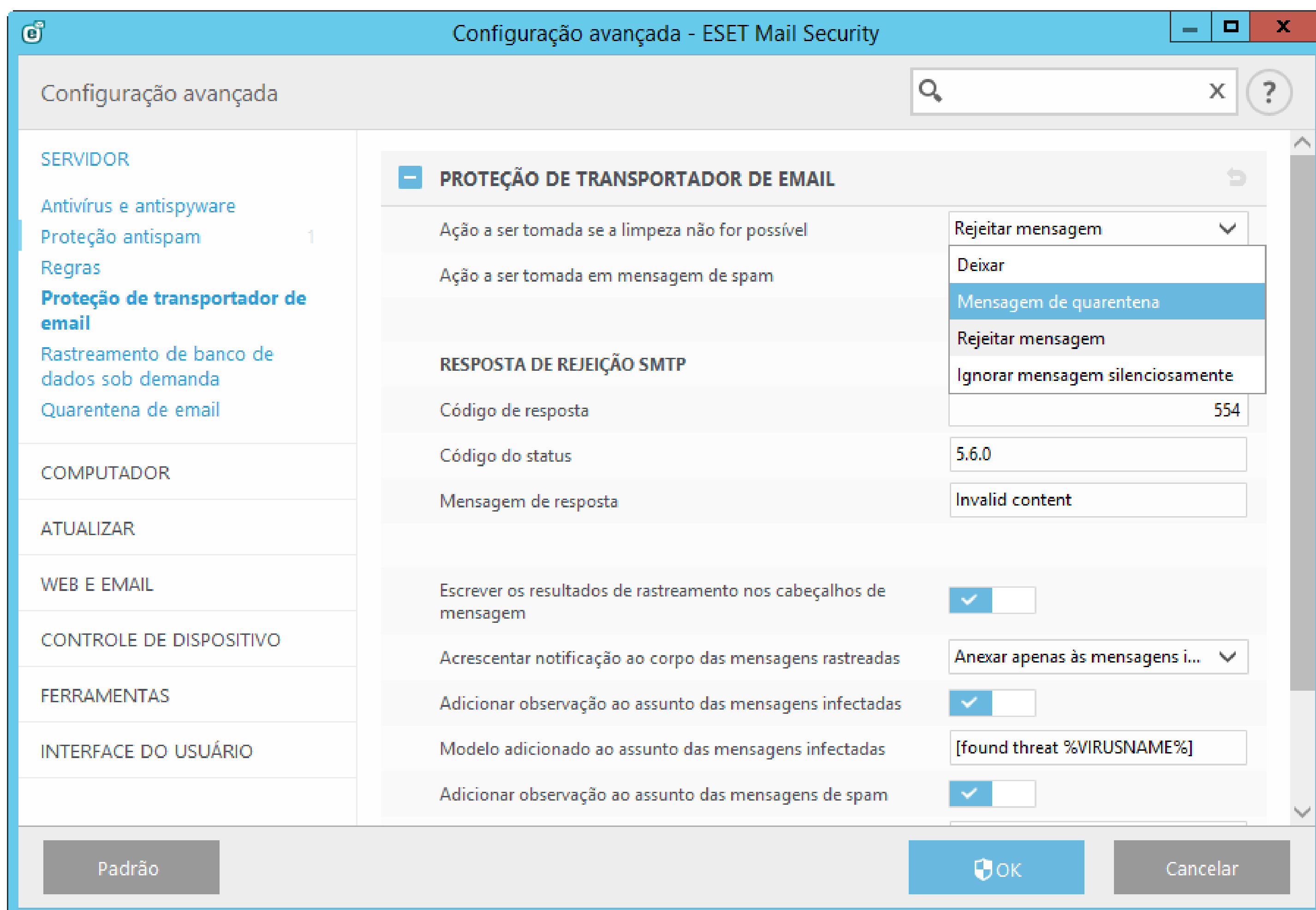
i **OBSERVAÇÃO**: Pastas públicas são tratadas da mesma forma que as caixas de entrada. Isso significa que pastas públicas também são rastreadas.

5.1.7 Proteção de transportador de email

Os sistemas operacionais a seguir têm **Proteção de transporte da caixa de entrada** disponível em **Configurações avançadas** > **Servidor**:

- Microsoft Exchange Server 2007 (Servidor Edge Transport ou Servidor Hub Transport)
- Microsoft Exchange Server 2007 (instalação de servidor única com várias funções)
- Microsoft Exchange Server 2010 (Servidor Edge Transport ou Servidor Hub Transport)
- Microsoft Exchange Server 2010 (instalação de servidor única com várias funções)
- Microsoft Exchange Server 2013 (função de servidor Edge Transport)
- Microsoft Exchange Server 2013 (instalação de servidor única com várias funções)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

Configurações de proteção do transporte de caixa de entrada:



A ação de antivírus na camada de transporte pode ser configurada em **Ação a ser tomada se a limpeza não for possível**:

- **Nenhuma ação -** manter a mensagem infectada que não pode ser limpa
- **Colocar mensagem em quarentena -** enviar as mensagens infectadas para a caixa de entrada de quarentena
- **Rejeitar mensagem -** rejeitar uma mensagem infectada
- **Ignorar mensagem silenciosamente** - excluir mensagens sem mandar um NDR (Relatório de não entrega)

A ação antispam na camada de transporte pode ser configurada em **Ação a ser tomada em mensagens de spam**:

- **Nenhuma ação** – mantém a mensagem mesmo que ela esteja marcada como spam
- **Colocar mensagem em quarentena** - envia mensagens marcadas como spam para a caixa de correio de quarentena
- **Rejeitar mensagem -** rejeita mensagens marcadas como SPAM
- **Ignorar mensagem silenciosamente** - exclui mensagens sem mandar um NDR (Relatório de não entrega)

Resposta de rejeição SMTP - é possível especificar um **Código de resposta**, **Código do status** e **Mensagem de resposta**, que definem a resposta de negação temporária de SMTP enviada para o servidor SMTP se uma mensagem for recusada.

Ao excluir mensagens, enviar resposta de rejeição SMTP:

- Se a opção estiver desmarcada, o servidor enviará a resposta SMTP OK para o MTA (Message Transfer Agent, Agente de Transferência de Mensagens) do remetente no formato '250 2.5.0 – Ação solicitada de email correta, concluída') e depois executará a remoção silenciosa.
- Se a opção estiver selecionada, uma resposta de rejeição SMTP será enviada de volta ao MTA do remetente. Você pode digitar uma mensagem de resposta no seguinte formato:

Código de resposta primária	Código de status complementar	Descrição

250	2.5.0	Ação solicitada de email correta, concluída
451	4.5.1	Ação solicitada anulada:erro local no processamento
550	5.5.0	Ação solicitada não executada:caixa de entrada indisponível
554	5.6.0	Conteúdo inválido

i **OBSERVAÇÃO:** Também é possível usar variáveis do sistema ao configurar Respostas de rejeição SMTP.

Acrescentar notificação ao corpo das mensagens rastreadas oferece três opções:
- Não anexar às mensagens
- Anexar apenas às mensagens infectadas
- Anexar a todas as mensagens rastreadas (não é aplicável a mensagens internas)

Adicionar observação ao assunto das mensagens infectadas - quando ativado, o ESET Mail Security vai anexar uma tag de notificação no assunto do email com o valor definido no campo de texto **Modelo adicionado ao assunto das mensagens de spam** (o texto padrão pré-definido é [SPAM]). Essa modificação pode ser usada para automatizar a filtragem de spam ao filtrar emails com um assunto específico, por exemplo, usando as regras ou, alternativamente, no lado do cliente (se for compatível com o cliente de email) colocar essas mensagens de email em uma pasta separada.

i **OBSERVAÇÃO:** Também é possível usar variáveis do sistema ao editar um texto que será adicionado ao assunto.

5.1.7.1 Configurações avançadas

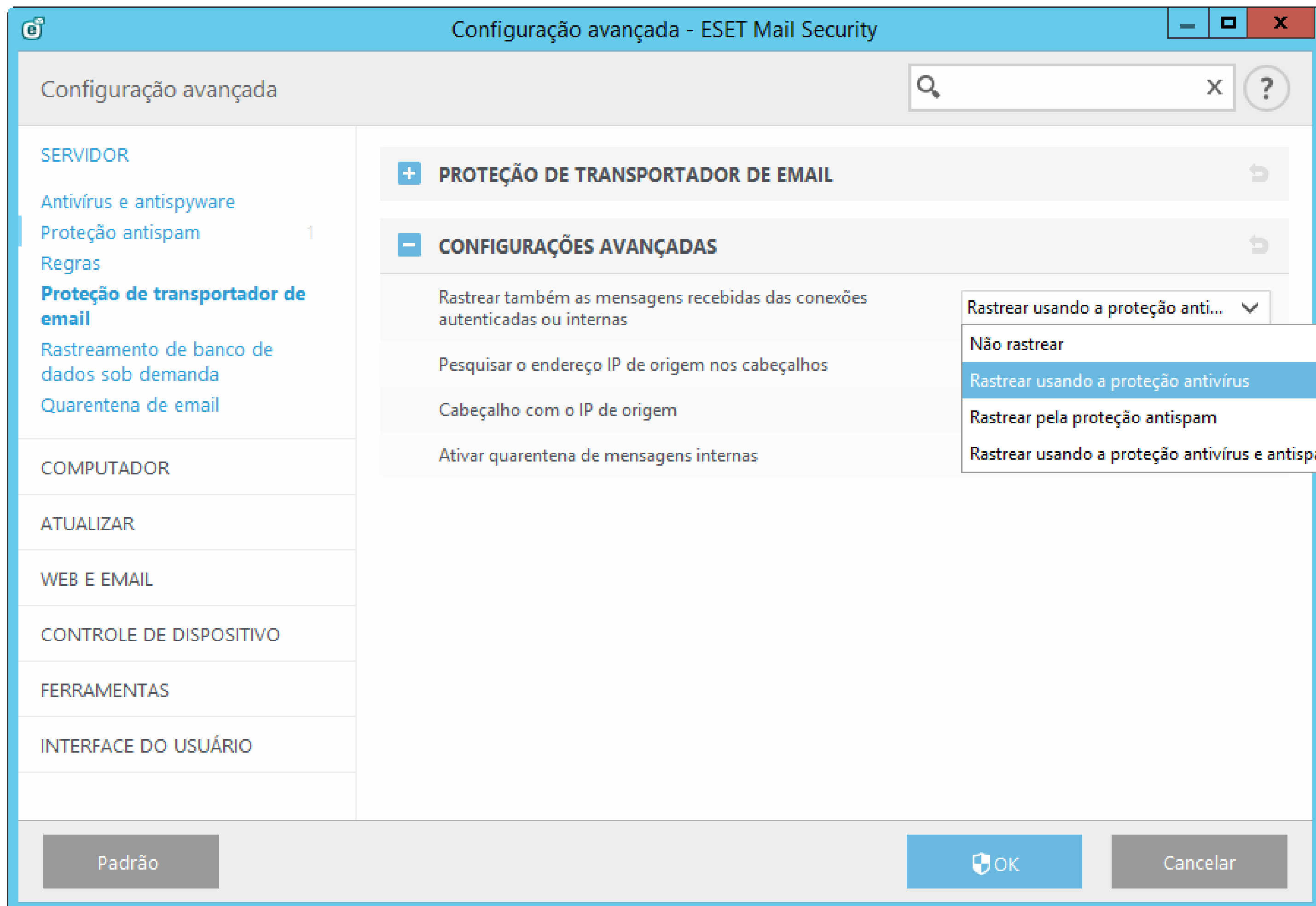
Nesta seção, você pode alterar as configurações avançadas aplicadas ao agente de transporte:

- **Rastrear também as mensagens recebidas das conexões autenticadas ou internas** - você pode escolher qual tipo de rastreamento deve ser realizado em mensagens recebidas de fontes autenticadas ou servidores locais. O rastreamento dessas mensagens é recomendado, pois aumenta a proteção, mas é necessário se você estiver usando um Microsoft SBS Conector POP3 integrado para buscar mensagens de emails a partir de servidores POP3 externos ou serviços de email (por exemplo **Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem**, etc.). Para mais informações veja Conector POP3 e antispam.

- **Pesquisar o endereço IP de origem nos cabeçalhos** - se ativado, o ESET Mail Security procura o endereço IP de origem no cabeçalho da mensagem para que módulos de proteção diferentes (Antispam e outros) possam usá-lo. Caso sua organização do Exchange seja separada da internet por um Proxy, Gateway ou servidor Edge Transport, massagens de email parecem chegar de um único endereço IP (normalmente um interno). É comum que, em servidores externos (por exemplo Edge Transport em DMZ), quando o endereço IP dos remetentes é conhecido, este endereço IP seja escrito no cabeçalho das mensagens de email que estão sendo recebidas. O calor especificado em **Cabeçalho com o IP de origem** abaixo é o cabeçalho que o ESET Mail Security busca em cabeçalhos de mensagens.

- **Cabeçalho com o IP de origem** - este é o cabeçalho que o ESET Mail Security procura em cabeçalhos de mensagem. O padrão é **X-Criando-IP**, mas se você estiver usando ferramentas de terceiros ou personalizadas que usam um cabeçalho diferente, altere o cabeçalho para um apropriado.

- **Ativar quarentena de mensagens internas** - quando ativado, mensagens internas serão colocadas em quarentena.



5.1.8 Rastreamento de banco de dados sob demanda

Lista de sistemas que tem o **Rastreamento de banco de dados sob demanda** disponível:

- Microsoft Exchange Server 2007 (Servidor Mailbox ou Servidor Hub Transport)
- Microsoft Exchange Server 2007 (instalação de servidor única com várias funções)
- Microsoft Exchange Server 2010 (Servidor Mailbox ou Servidor Hub Transport)
- Microsoft Exchange Server 2010 (instalação de servidor única com várias funções)
- Microsoft Exchange Server 2013 (função de servidor Mailbox)
- Microsoft Exchange Server 2013 (instalação de servidor única com várias funções)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

OBSERVAÇÃO: Se estiver executando o Microsoft Exchange Server 2007 ou 2010 é possível escolher entre o rastreamento de Proteção do banco de dados da caixa de entrada e Banco de dados sob demanda. Porém, apenas um tipo de proteção entre esses dois pode estar ativo por vez. Se decidir usar o rastreamento de banco de dados sob demanda, será preciso desativar a integração da Proteção do banco de dados da caixa de entrada na Configuração avançada, em Servidor. Caso contrário o Rastreamento de banco de dados sob demanda não estará disponível.

Configurações de rastreamento de banco de dados sob demanda:

Endereço de host - Nome ou endereço IP do servidor executando o EWS (Serviços da web do Exchange).

Nome de usuário - Especifique as credenciais para um usuário que tem acesso adequado ao EWS (Serviços da web do Exchange).

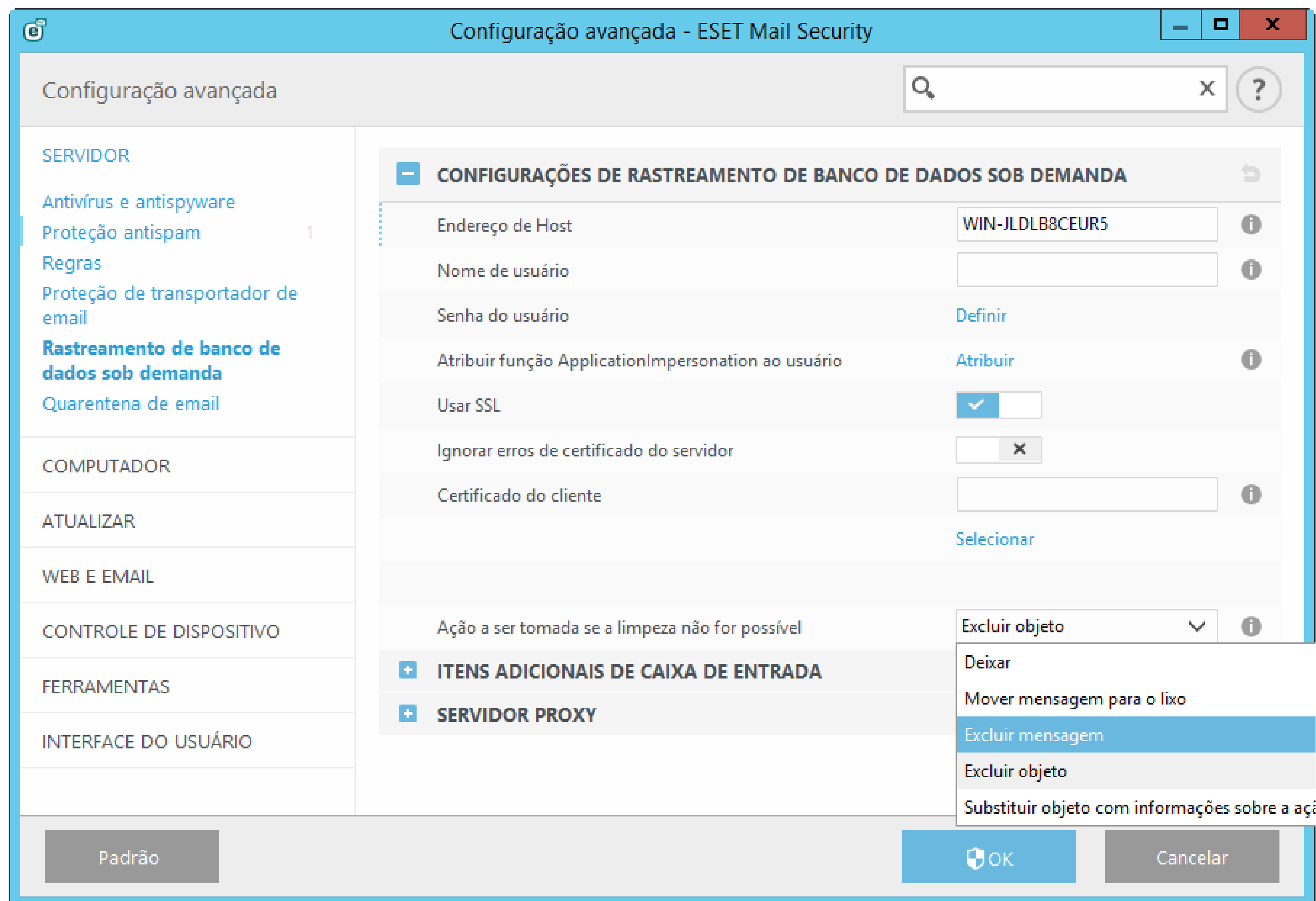
Senha do usuário - Clique em **Definir** ao lado de **Senha do usuário** e digite a senha para esta conta do usuário.

Atribuir função ApplicationImpersonation ao usuário - Clique em **Atribuir** para atribuir automaticamente função de ApplicationImpersonation ao usuário selecionado.

Usar SSL - precisa estar ativado se EWS (Serviços da web do Exchange) estiver configurado como **Requer SSL** no IIS. Se SSL estiver ativado, o certificado do Exchange Server deve ser importado para o sistema com o ESET Mail Security (caso as funções do Exchange Server estejam em servidores diferentes). Configurações para o EWS podem ser encontradas em IIS em *Configurações de Sites/Site padrão/EWS/SSL*.

OBSERVAÇÃO: Desative **Usar SSL** somente se o EWS estiver configurado em IIS para não Solicitar SSL.

Certificado do cliente - precisa ser definido apenas quando os Serviços da web do Exchange solicitarem certificado do cliente. **Selecionar** permite selecionar qualquer um dos certificados.



Ação a ser tomada se a limpeza não for possível - este campo de ações permite **bloquear** conteúdo infectado.

Nenhuma ação - não executa nenhuma ação no conteúdo infectado da mensagem.
Mover mensagem para o Lixo - não é compatível com itens da Pasta Pública. A ação **Excluir objeto** será aplicada em seu lugar.
Excluir objeto - conteúdo infectado da mensagem.
Excluir mensagem - exclui a mensagem inteira, incluindo o conteúdo infectado.
Substituir objeto com informações sobre a ação - remove um objeto e coloca informações sobre a ação que foi realizada com este objeto.

5.1.8.1 Itens adicionais de caixa de entrada

Configurações de rastreamento de banco de dados sob demanda permite que você ative ou desative a verificação de outros tipos de itens da caixa de entrada:

- Rastrear calendário
- Rastrear tarefas
- Rastrear contatos
- Rastrear agenda

OBSERVAÇÃO: Se você tiver problemas de desempenho, você pode desativar o rastreamento desses itens. Rastreamentos vão demorar mais tempo quando esses itens estão ativados.

5.1.8.2 Servidor proxy

Caso esteja usando um servidor proxy entre seu Exchange Server com função CAS e Exchange Server onde o ESET Mail Security está instalado, especifique os parâmetros de seu servidor proxy. Isto é necessário porque o ESET Mail Security conecta com o API EWS (Serviços da web do Exchange) via HTTP/HTTPS. Caso contrário o Rastreamento de banco de dados sob demanda não vai funcionar.

Servidor proxy - digite o endereço IP ou nome do servidor proxy que você usar.

Porta - digite o número da porta do servidor proxy.

Nome de usuário, Senha - digite as credenciais se o seu servidor proxy requisitar autenticação.

5.1.8.3 Detalhes da conta de rastreamento de banco de dados

Essa janela de diálogo será exibida se você não tiver especificado um nome de usuário e senha para o **Rastreamento de banco de dados** na **Configuração avançada**. Especifique as credenciais do usuário que tem acesso ao EWS (Serviços da web do Exchange) nesta janela pop-up e clique em **OK**. Alternativamente, vá para **Configuração avançada** pressionando **F5** e navegue até **Servidor** > Rastreamento de banco de dados sob demanda. Digite seu **Nome de usuário**, clique em **Definir**, digite uma senha para esta conta de usuário e clique em OK.

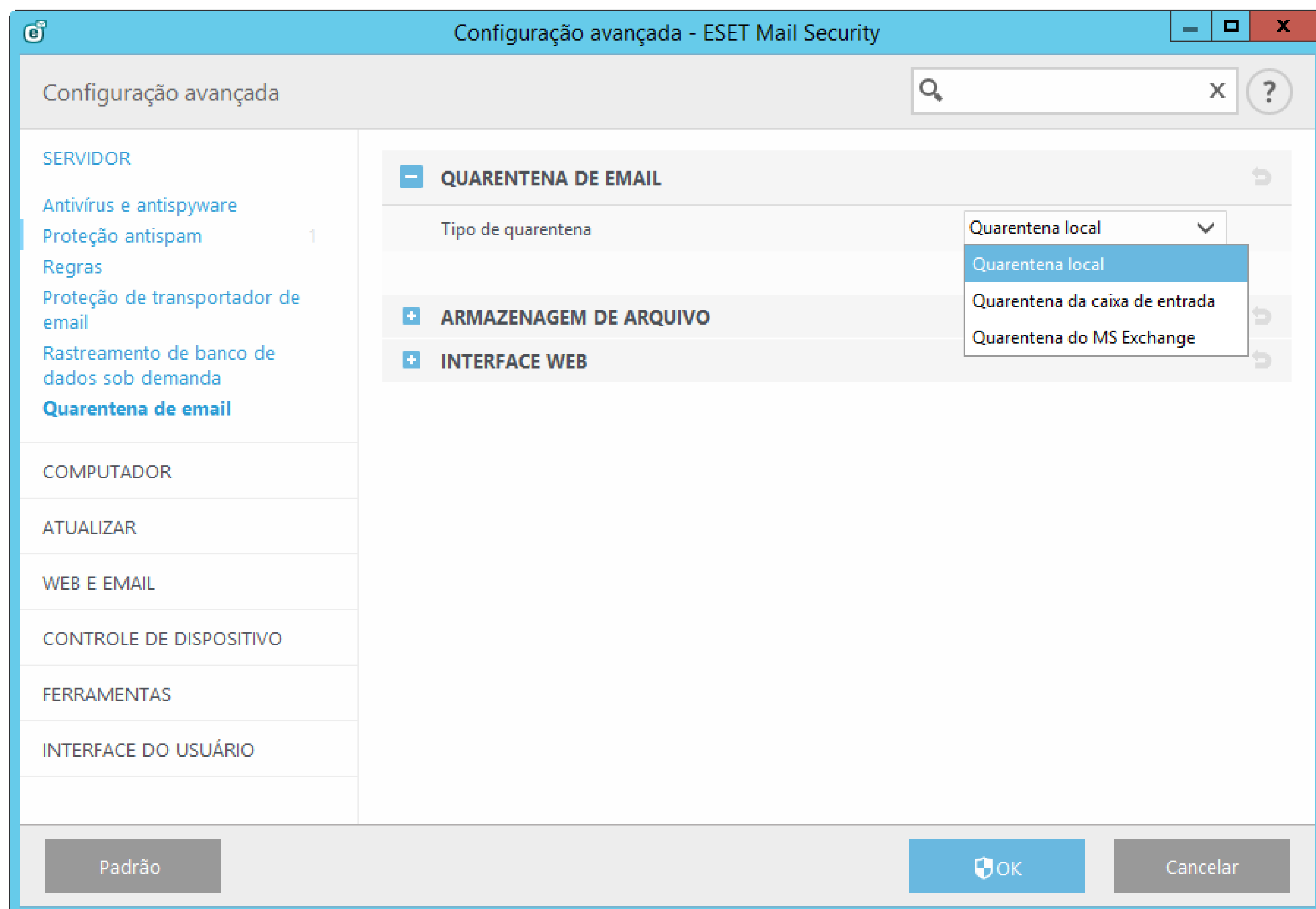
- Você pode selecionar **Salvar informações de conta** para salvar as configurações da conta, assim você não terá que digitar as informações da conta cada vez que executar um Rastreamento de banco de dados sob demanda.
- Se uma conta de usuário não tiver acesso adequado a EWS, você pode selecionar **Criar atribuição de função "ApplicationImpersonation"** para atribuir essa função a uma conta.

Database scan account details
Scan account details
User name
FRANTO\administrator
Password
Save account information
Create "ApplicationImpersonation" role assignment
OK
Cancel

5.1.9 Quarentena de email

O gerente de quarentena de email está disponível para todos os três tipos de quarentena:

- Quarentena local
- Quarentena da caixa de entrada
- Quarentena do MS Exchange



Você pode ver o conteúdo da Quarentena de email no Gerente de quarentena de email para todos os tipos de Quarentena. Além disso, a quarentena local também pode ser vista na Interface web de quarentena de email.

5.1.9.1 Quarentena local

A quarentena local usa o sistema de arquivos local para armazenar emails em quarentena e um banco de dados SQLite como um índice. Arquivos de email em quarentena armazenados, assim como arquivos de banco de dados, são criptografados por razões de segurança. Esses arquivos estão localizados em `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (no Windows Server 2008 e 2012) ou `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (no Windows Server 2003).

Recursos de quarentena Locais:

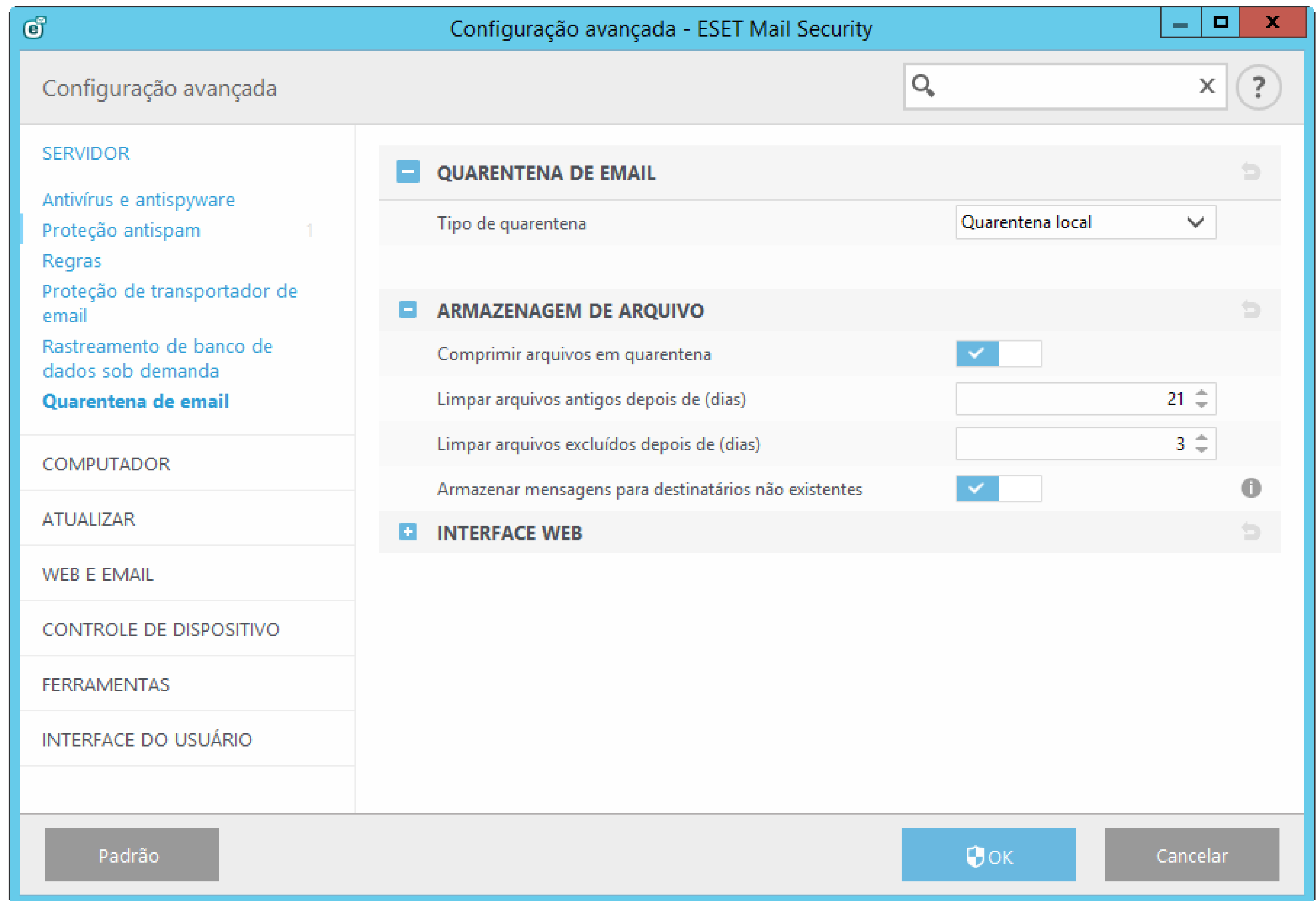
- Criptografia e compressão de arquivos de email armazenados em quarentena.
- Arquivos de email em quarentena removidos da janela de quarentena (por padrão, depois de 21 dias) ainda estão armazenados em um sistema de arquivos (até que a exclusão automática ocorre depois de um determinado número de dias)
- Exclusão automática de arquivos de email antigos (o padrão é depois de 3 dias). Para mais informações consulte as configurações de Armazenamento de arquivos.
- Você pode restaurar arquivos de email em quarentena removidos usando o eShell (assumindo que eles ainda não foram excluídos do sistema de arquivos).

Você pode inspecionar mensagens de email em quarentena e decidir **excluir** ou **lançar** qualquer uma delas. Para

visualizar e gerenciar localmente mensagens de email em quarentena, você pode usar o Gerente de quarentena de email a partir da interface gráfica do usuário principal ou a Interface web de Quarentena de email.

5.1.9.1.1 Armazenagem de arquivo

Nesta seção você pode alterar as configurações para armazenamento de arquivos usadas pela quarentena local.



Comprimir arquivos em quarentena - os arquivos em quarentena comprimidos ocupam menos espaço em disco, mas se você decidir não ter arquivos compactados, use o botão para desativar a compressão.

Limpar arquivos antigos depois de (dias) - quando as mensagens alcançam o número de dias especificado, elas são removidas da janela de quarentena. Porém, os arquivos não serão excluídos do disco pela quantidade de dias especificada em **Limpar arquivos excluídos depois de (dias)**. Como os arquivos não são excluídos do sistema de arquivos, é possível recuperar esses arquivos usando o eShell.

Limpar arquivos excluídos depois de (dias) - exclui arquivos do disco depois do número de dias especificado, não é possível recuperar depois de serem excluídos (a menos que você tenha uma solução de backup do sistema de arquivos implementada).

Armazenar mensagens para destinatários não existentes - normalmente mensagens de spam são enviadas a destinatários aleatórios para um determinado domínio em uma tentativa de acertar um usuário já existente. As mensagens enviadas para usuários que não existem em um Active Directory são armazenadas na quarentena local por padrão. Mas isso pode ser desligado e mensagens para destinatários inexistentes não serão armazenadas, assim sia Quarentena local não ficará cheia com muitas mensagens de spam deste tipo. Isto também economiza espaço em disco.

5.1.9.1.2 Interface web

A Interface web da Quarentena de email é uma alternativa ao Gerente de quarentena de email, mas só está disponível para a Quarentena local.

OBSERVAÇÃO: A Interface web de Quarentena de email não está disponível em um servidor com função de servidor Edge Transport. Isso acontece porque o Active Directory não está acessível para autenticação.

A Interface web da Quarentena de email permite que você veja o estado da quarentena de email. Ela também permite que você gerencie objetos de email em quarentena. Esta interface web pode ser acessada através de links de relatórios de quarentena ou diretamente, digitando um URL em um navegador da web. Para acessar a interface web da Quarentena de email, você deve autenticar usando credenciais de domínio. O Internet Explorer irá autenticar automaticamente para um usuário do domínio, o certificado da página web deve ser válido, Logon automático deve estar ativado no IE e você deve adicionar o site da Quarentena de email nos sites da intranet local.

O botão **Ativar interface da web** permite desativar ou ativar a interface web.

Lançamento - lança o email ao seu destinatário original usando o diretório de reprodução, e exclui o email da quarentena. Clique em **Enviar** para confirmar a ação.
Excluir - exclui itens da quarentena. Clique em **Enviar** para confirmar a ação.

Quando clicar em **Assunto**, uma janela pop-up será aberta com detalhes sobre o email em quarentena como **Tipo**, **Motivo**, **Remetente**, **Data**, **Anexos**, etc.

Quarantined mail detail

TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28
ATTACHMENTS	

Show headers

RELEASE DELETE Go to quarantine view.

Clique em **Mostrar cabeçalhos** para revisar o cabeçalho da quarentena.

Quarantined mail detail

TYPE	spam
REASON	Found GTUBE test string
SUBJECT	hlavicka
SENDER	test@test.sk
SMTP RECIPIENTS	vista@s2.local
TO	vista@s2.local
CC	
DATE	2015-06-22 23:28
ATTACHMENTS	

```
Received: from win2k3r2x64-ss4 ([10.1.117.232]) by win2k3sp2x86ss1.s2.local with Microsoft SMTPSVC(6.0.3790.4675);
        Mon, 22 Jun 2015 23:28:46 -0700
Received:
To: <vista@s2.local>
Subject:[SPAM] hlavicka
X-Originating-IP:
MIME-Version: 1.0
Content-Type: text/plain
Message-ID: <-974233353.8808@win2k8x64-EDGE.s1.local>
From:
Return-Path: < >
Date: Tue, 9 Nov 2010 22:12:48 -0800
X-MS-Exchange-Organization-OriginalArrivalTime: 10 Nov 2010 06:12:48.9975
 (UTC)
X-MS-Exchange-Organization-AuthSource: win2k8x64-EDGE.s1.local
X-MS-Exchange-Organization-AuthAs: Anonymous
Received-SPF: Fail (win2k8x64-EDGE.s1.local: domain of  does not designate
 10.1.117.225 as permitted sender) receiver=win2k8x64-EDGE.s1.local;
```

RELEASE DELETE Go to quarantine view.

Se quiser, clique em **Lançar** ou **Excluir** para realizar uma ação com uma mensagem de email em quarentena.

i **OBSERVAÇÃO**: Você deve fechar a janela do navegador para fazer logout completamente da interface Web da Quarentena de email. Caso contrário, clique em **Ir** para que a vista de quarentena volte para a tela anterior.

You must close your browser to complete the sign out process.

Go to quarantine view.

Importante: Se estiver tendo problemas para acessar a interface da web da Quarentena de email do seu navegador ou estiver recebendo o erro `Erro HTTP 403.4 - Proibido` ou similar, verifique qual Tipo de quarentena está selecionado e certifique-se de que é a **Quarentena local** e que **Ativar interface da web** está ativado.

5.1.9.2 Quarentena da caixa de entrada e quarentena do MS Exchange

Se você decidir não usar a Quarentena local você tem duas opções, ou a **Quarentena da caixa de entrada** ou a **Quarentena do MS Exchange**. Independentemente da opção escolhida, você precisa criar um usuário dedicado com caixa de entrada (por exemplo main_quarantine@company.com) que será usado para armazenar mensagens de email em quarentena. Este usuário e caixa de entrada também serão usados pelo Gerente de quarentena de email para visualizar e gerenciar itens na quarentena. Você vai precisar especificar os detalhes da conta deste usuário nas Configurações do gerente de quarentena.

Importante: Não recomendamos usar a conta de usuário Administrador como caixa de entrada de quarentena.

OBSERVAÇÃO: **Quarentena do MS Exchange** não está disponível para o Microsoft Exchange 2003, apenas a **Quarentena local** e **Quarentena da caixa de entrada**.

- Quando você seleciona a **Quarentena do MS Exchange**, o ESET Mail Security vai usar o **sistema de quarentena do Microsoft Exchange** (isso se aplica ao Microsoft Exchange Server 2007 e versões mais recentes). Nesse caso, o mecanismo interno do Exchange é usado para armazenar mensagens potencialmente infectadas e SPAM.

OBSERVAÇÃO: Por padrão, a quarentena interna não está ativada no Exchange. Para ativá-la, é necessário abrir o Exchange Management Shell e digitar o seguinte comando (substitua `name@domain.com` pelo endereço real de sua caixa de entrada dedicada):

```
Set-ContentFilterConfig -QuarantineMailbox name@domain.com
```

- Ao selecionar a **Caixa de entrada de quarentena**, você precisa especificar o endereço de quarentena da mensagem (por exemplo main_quarantine@company.com).

5.1.9.2.1 Configurações do gestor de quarentena

Endereço de host - vai aparecer automaticamente se o Exchange Server com função CAS estiver presente no local. Alternativamente, se a função CAS não estiver presente no mesmo servidor com o ESET Mail Security instalado, mas ela pode ser encontrada dentro do AD, endereço de host aparecerá automaticamente. Se não aparecer, você pode digitar o nome do host manualmente. A detecção automática não funcionará na função de servidor Edge Transport.

OBSERVAÇÃO: O endereço IP não é compatível, você precisa usar o nome do host do servidor CAS.

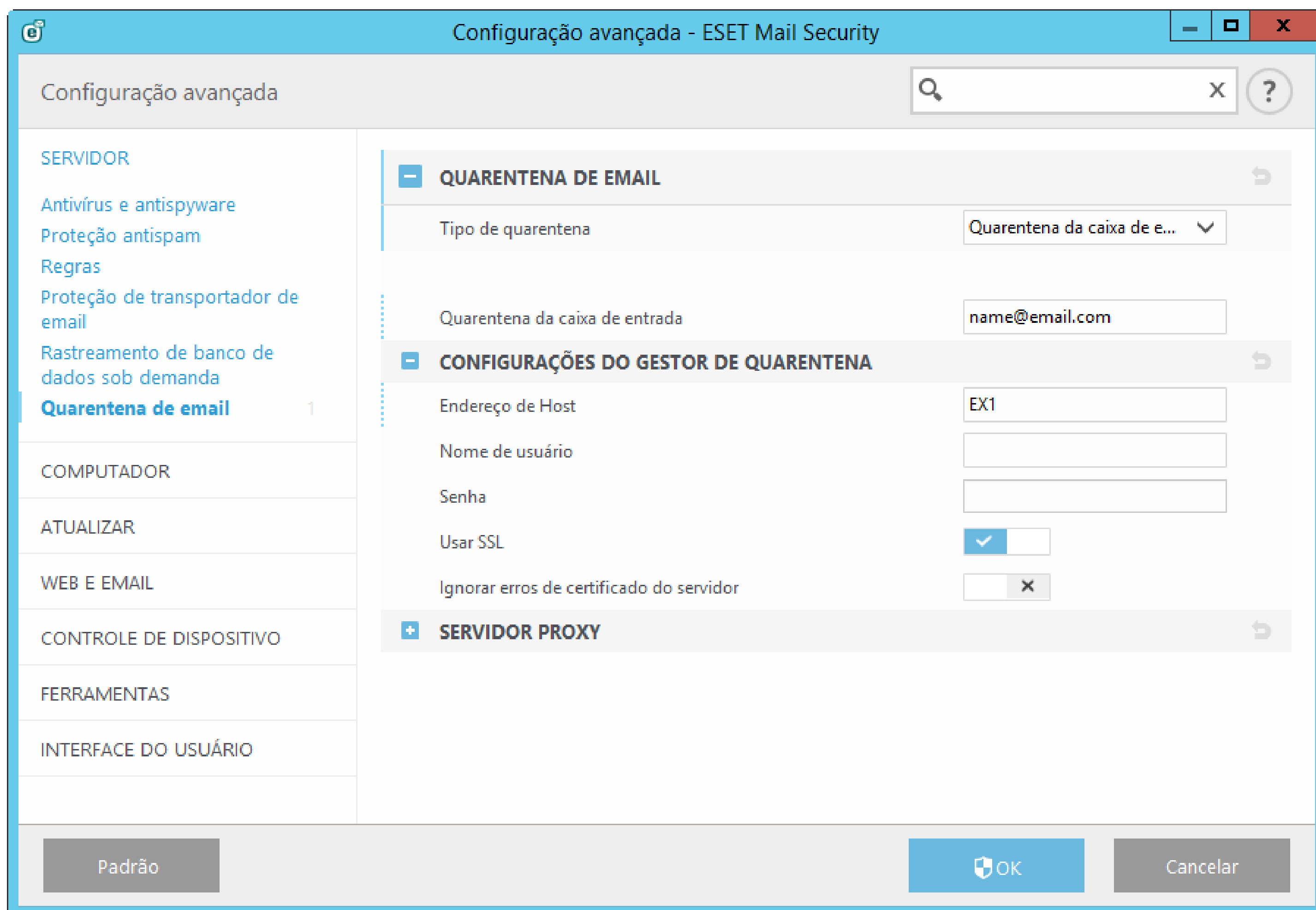
Nome de usuário - conta de usuário de quarentena dedicada que você criou para armazenar mensagens em quarentena (ou uma conta que tem acesso a essa caixa de entrada através de delegação de acesso). Na função de servidor do Edge Transport que não faz parte do domínio, é necessário usar o endereço de email inteiro (por exemplo main_quarantine@company.com).

Senha - digite a senha da sua conta de quarentena.

Usar SSL - precisa estar ativado se EWS (Serviços da web do Exchange) estiver configurado como **Requer SSL** no IIS. Se SSL estiver ativado, o certificado do Exchange Server deve ser importado para o sistema com o ESET Mail Security (caso as funções do Exchange Server estejam em servidores diferentes). Configurações para o EWS podem ser encontradas em IIS em *Configurações de Sites/Site padrão/EWS/SSL*.

OBSERVAÇÃO: Desative **Usar SSL** somente se o EWS estiver configurado em IIS para não Solicitar SSL.

Ignorar erros de certificado do servidor - Ignora os estados a seguir: auto assinado, nome errado no certificado, uso errado, expirado.



5.1.9.2.2 Servidor proxy

Caso esteja usando um servidor proxy entre seu Exchange Server com função CAS e Exchange Server onde o ESET Mail Security está instalado, especifique os parâmetros de seu servidor proxy. Isto é necessário porque o ESET Mail Security conecta com o API EWS (Serviços da web do Exchange) via HTTP/HTTPS. Caso contrário, a caixa de entrada de quarentena e a quarentena do MS Exchange não vão funcionar.

Servidor proxy - digite o endereço IP ou nome do servidor proxy que você usar.

Porta - digite o número da porta do servidor proxy.

Nome de usuário, Senha - digite as credenciais se o seu servidor proxy requisitar autenticação.

5.1.9.3 Detalhes da conta do gerente de quarentena

Essa janela de diálogo será exibida se você não configurar uma conta para seus **Detalhes do gerente de quarentena**. Especifique as credenciais para um usuário com acesso a **Caixa de entrada de quarentena** e clique em **OK**. Alternativamente, pressione F5 para acessar a **Configuração avançada** e vá até **Servidor** > **Quarentena de email** > Configurações do gerente de quarentena. Digite o **Nome de usuário** e **Senha** para sua caixa de entrada de quarentena.

Você pode selecionar **Salvar informações de conta** para salvar as configurações de conta para uso futuro quando acessar o Gerente de quarentena.

5.1.10 Agrupamento

O **Agrupamento ESET** é uma infraestrutura de comunicação P2P da linha de produtos ESET para o Microsoft Windows Server.

Esta infraestrutura permite que os produtos de servidor da ESET se comuniquem uns com os outros e troquem dados como configurações e notificações, e também que sincronizem os dados necessários para a operação correta de um grupo de instâncias do produto. Um exemplo de tal grupo é um grupo de nós em um Agrupamento de Failover Windows ou Agrupamento de Balanceamento de Carga de Rede (NLB) com produto ESET instalado onde há necessidade de ter a mesma configuração do produto em todo o agrupamento. O Agrupamento ESET garante esta uniformidade entre instâncias.

A página de status do Agrupamento ESET pode ser acessada no menu principal em **Ferramentas** > **Agrupamento** quando configurada adequadamente, a página deve ter a seguinte aparência:

Para configurar o Agrupamento ESET, clique em **Assistente do agrupamento...** Para detalhes sobre como configurar o Agrupamento ESET usando o assistente, clique aqui.

Ao configurar o Agrupamento ESET existem duas formas de adicionar nós - automaticamente usando o Agrupamento de Failover Windows / Agrupamento NLB ou manualmente ao procurar computadores que estejam em um Grupo de trabalho ou em um Domínio.

Detectar automaticamente - detecta automaticamente nós que já fazem parte de um Agrupamento de Failover Windows / Agrupamento NLB e adiciona estes a um Agrupamento ESET
Procurar - É possível adicionar nós manualmente ao digitar os nomes do servidor (que sejam ou membros do mesmo Grupo de trabalho ou membros do mesmo Domínio)

OBSERVAÇÃO: O servidor não precisa fazer parte de um Agrupamento de Failover Windows / Agrupamento NLB para usar o recurso Agrupamento ESET. Um Agrupamento de Failover Windows ou Agrupamento NLB não precisa estar instalado em seu ambiente para usar os agrupamentos ESET.

Assim que os nós tiverem sido adicionados ao seu Agrupamento ESET, a próxima etapa é a instalação do ESET Mail Security em cada nó. Isto é feito automaticamente durante a configuração do Agrupamento ESET.

Credenciais necessárias para a instalação remota do ESET Mail Security em outros nós de agrupamento:

- Cenário de Domínio - credenciais do administrador de domínio
- Cenário do grupo de trabalho - é preciso certificar-se de que todos os nós usam as mesmas credenciais de conta do administrador local

Em um Agrupamento ESET também é possível usar uma combinação de nós adicionados automaticamente como membros de um Agrupamento de Failover Windows / Agrupamento NLB existente e nós adicionados manualmente (desde que estejam no mesmo Domínio).

i **OBSERVAÇÃO:** Não é possível combinar nós de Domínio com nós de Grupo de trabalho.

Outro requisito do Agrupamento ESET é que **Compartilhamento de arquivos e impressora** deve estar ativado no Firewall do Windows antes de fazer a instalação do ESET Mail Security nos nós do Agrupamento ESET.

O Agrupamento ESET pode ser desfeito facilmente clicando em **Destruir agrupamento**. Cada nó vai escrever um registro do seu relatório de eventos sobre o Agrupamento ESET ser destruído. Depois disso, todas as regas de firewall ESET são retiradas do Firewall do Windows. Nós anteriores serão revertidos no seu estado anterior e podem ser usados novamente em outro Agrupamento ESET se necessário.

i **OBSERVAÇÃO:** A criação de Agrupamentos ESET entre o ESET Mail Security e o ESET File Security para Linux não é compatível.

Adicionar novos nós a um Agrupamento ESET existente pode ser feito a qualquer momento ao executar o **Assistente do agrupamento** da mesma forma descrita acima e aqui.

Veja a seção Agrupamento de trabalho para mais informações sobre a configuração de agrupamento ESET.

5.1.10.1 Assistente do agrupamento - página 1

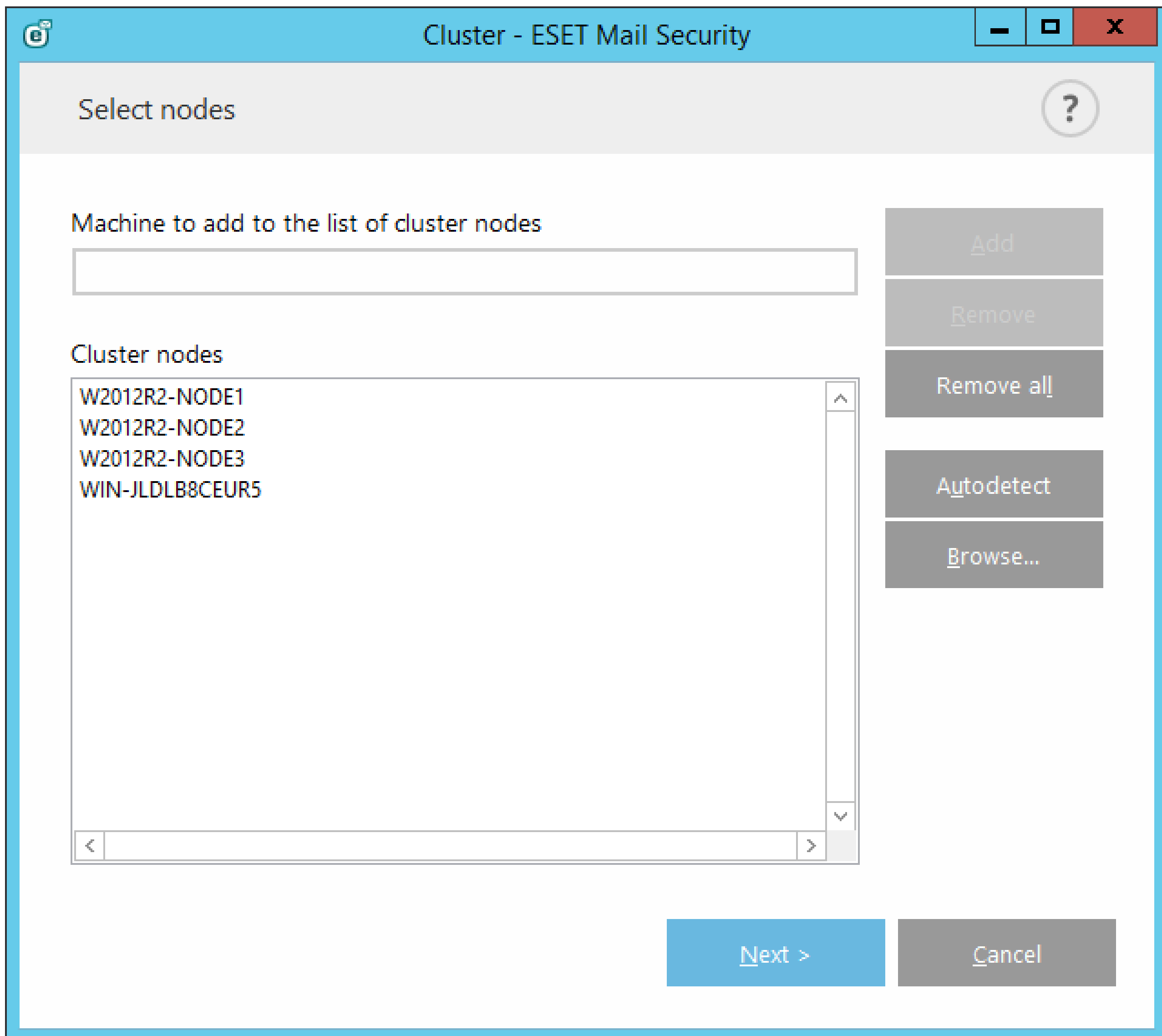
A primeira etapa ao configurar um Agrupamento ESET é adicionar nós. Você pode usar a opção **Detectar automaticamente** ou **Procurar** para adicionar nós. Como uma alternativa, você pode digitar o nome do servidor na caixa de texto e clicar em **Adicionar**.

Detectar automaticamente adiciona automaticamente nós de um Agrupamento de Failover Windows / Agrupamento de Balanceamento de Carga de Rede (NLB) existente. O servidor sendo usado para criar o Agrupamento ESET precisa ser um membro deste Agrupamento de Failover Windows / Agrupamento NLB para detectar automaticamente os nós. O Agrupamento NLB deve ter o recurso **Permitir controle remoto** ativado em propriedades de agrupamento para o Agrupamento ESET detectar os nós corretamente. Assim que você tiver a lista dos nós adicionados recentemente, é possível remover os indesejados, caso você queira apenas nós específicos no Agrupamento ESET.

Clique em **Procurar** para encontrar e selecionar computadores dentro de um Domínio ou Grupo de trabalho. Este método permite a adição manual de nós no Agrupamento ESET.

Outra forma de adicionar nós é digitar o nome do host do servidor que deseja adicionar e clicar em **Adicionar**.

Nós de agrupamento atuais escolhidos para serem adicionados ao Agrupamento ESET depois de clicar em **Avançar**:



Para modificar os **Nós de agrupamento** da lista, selecione o nó que você deseja remover e clique em **Remover** ou, para apagar a lista completamente, clique em **Remover tudo**.

Se você já tiver um Agrupamento ESET existente, é possível adicionar novos nós a ele a qualquer momento. As etapas são as mesmas descritas acima.

OBSERVAÇÃO: Todos os nós que continuam na lista devem estar on-line e poderem ser alcançados. O host local é adicionado aos Nós de agrupamento por padrão.

5.1.10.2 Assistente do agrupamento - página 2

Defina um nome de agrupamento, modo de distribuição de certificado e se o produto será instalado nos outros nós ou não.

Cluster - ESET Mail Security

Cluster name and install type

Cluster name

clusterName

Listening port

9777

Open port in Windows firewall

Certificate distribution

Automatic remote

Manual

Generate...

Product installation on other nodes

Automatic remote

Manual

Push license to nodes without activated product

< Previous Next > Cancel

Nome do agrupamento - digite o nome do seu agrupamento.
Porta de escuta - (a porta padrão é 9777)
Porta aberta no firewall do Windows - quando marcado, uma regra é criada no Firewall do Windows.

Distribuição de certificado:
Remoto automático - o certificado será instalado automaticamente.
Manual- ao clicar em **Gerar** uma janela de navegação será aberta - selecione a pasta onde armazenar os certificados. Um Certificado raiz assim como um certificado para cada nó será criado, incluindo o nó (máquina local) de onde você está configurando o Agrupamento ESET. Então é possível escolher inscrever o certificado na máquina local ao clicar em **Sim**. Mais tarde será necessário importar certificados manualmente conforme descrito aqui.

Instalar produto em outros nós:
Remoto automático - ESET Mail Security será instalado automaticamente em cada nó (desde que seus sistemas operacionais tenham a mesma arquitetura).
Manual - escolha este se quiser instalar o ESET Mail Security manualmente (por exemplo, quando você tem arquiteturas de sistema operacional diferentes em alguns nós).

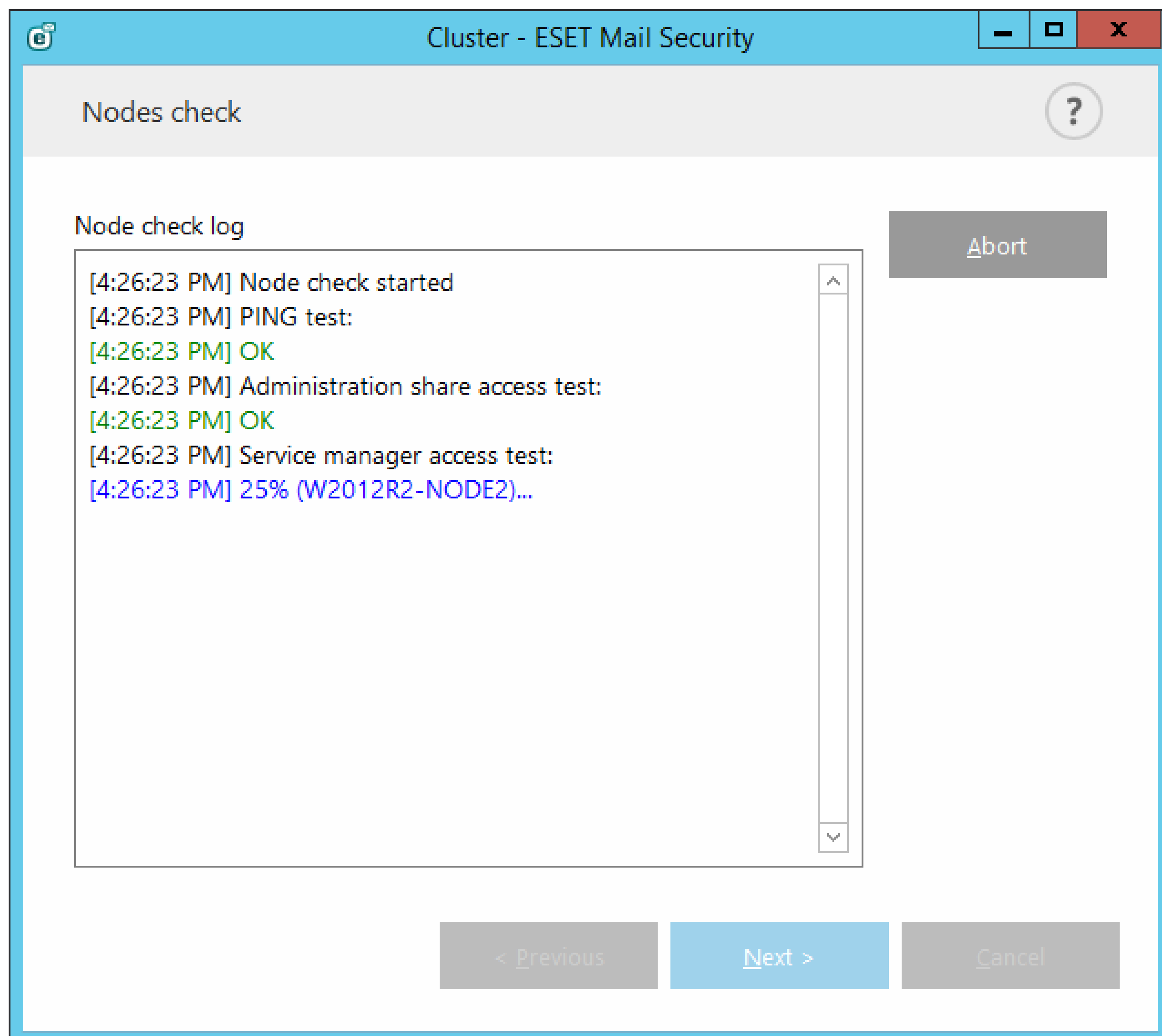
Empurrar licença para os nós sem o produto ativado - quando estiver marcado, os nós ativarão o ESET Mail Security.

i **OBSERVAÇÃO:** Se quiser criar um Agrupamento ESET com arquiteturas mistas de sistema operacional (32 bit e 64 bit) será preciso instalar o ESET Mail Security manualmente. Isto será detectado durante as próximas etapas e você verá estas informações na janela de relatório.

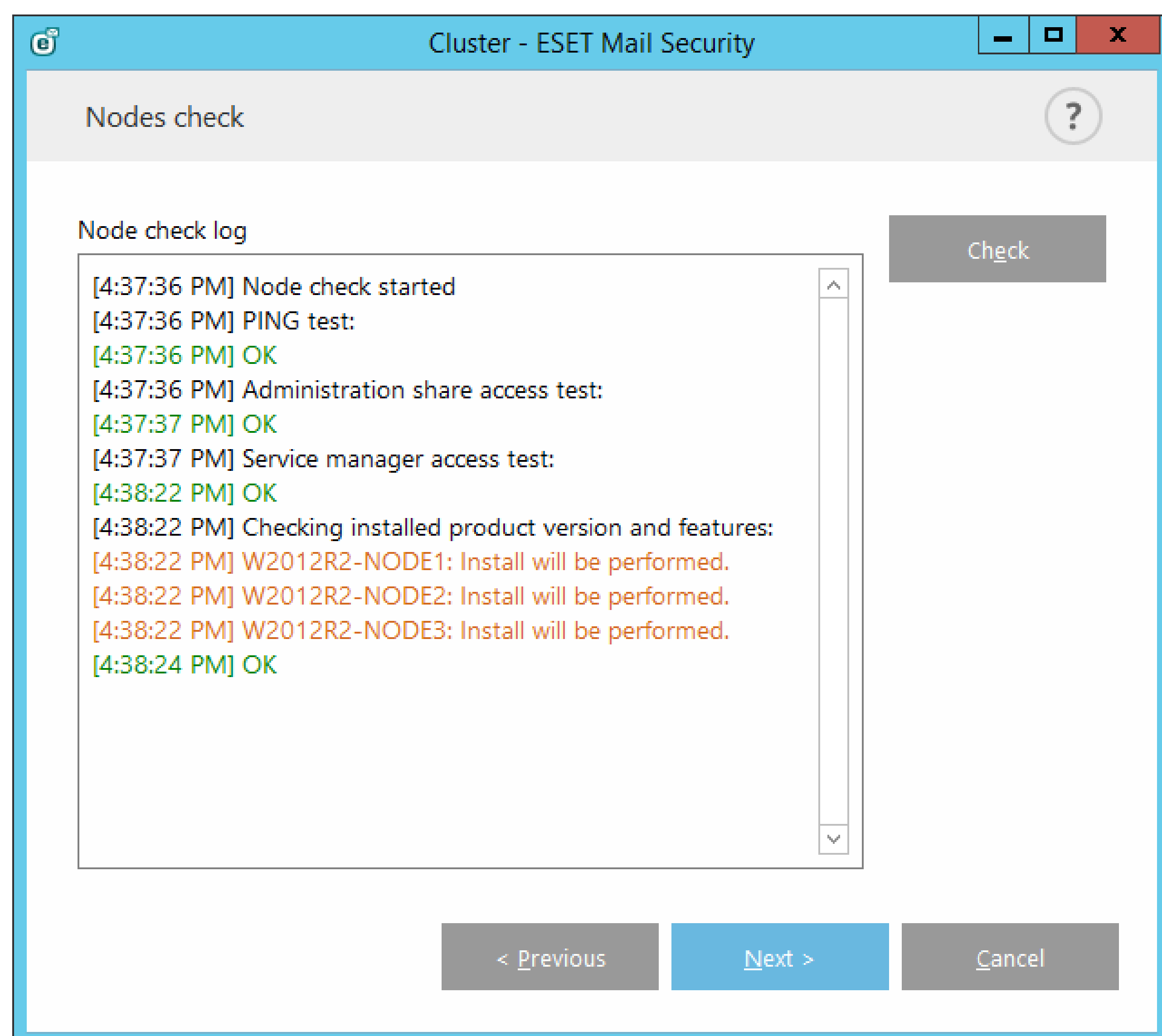
5.1.10.3 Assistente do agrupamento - página 3

Depois de especificar os detalhes de instalação, uma verificação de nó é executada. Você verá o seguinte ser verificado no **Relatório de verificação de nós**:

- verificar se todos os nós existentes estão on-line
- verificar se todos os nós podem ser acessados
- o nó está on-line
- o compartilhamento de admin pode ser acessado
- a execução remota é possível
- a versão correta do produto está instalada, ou não há produto (apenas se a instalação automática estiver selecionada)
- verificar se os novos certificados estão presentes

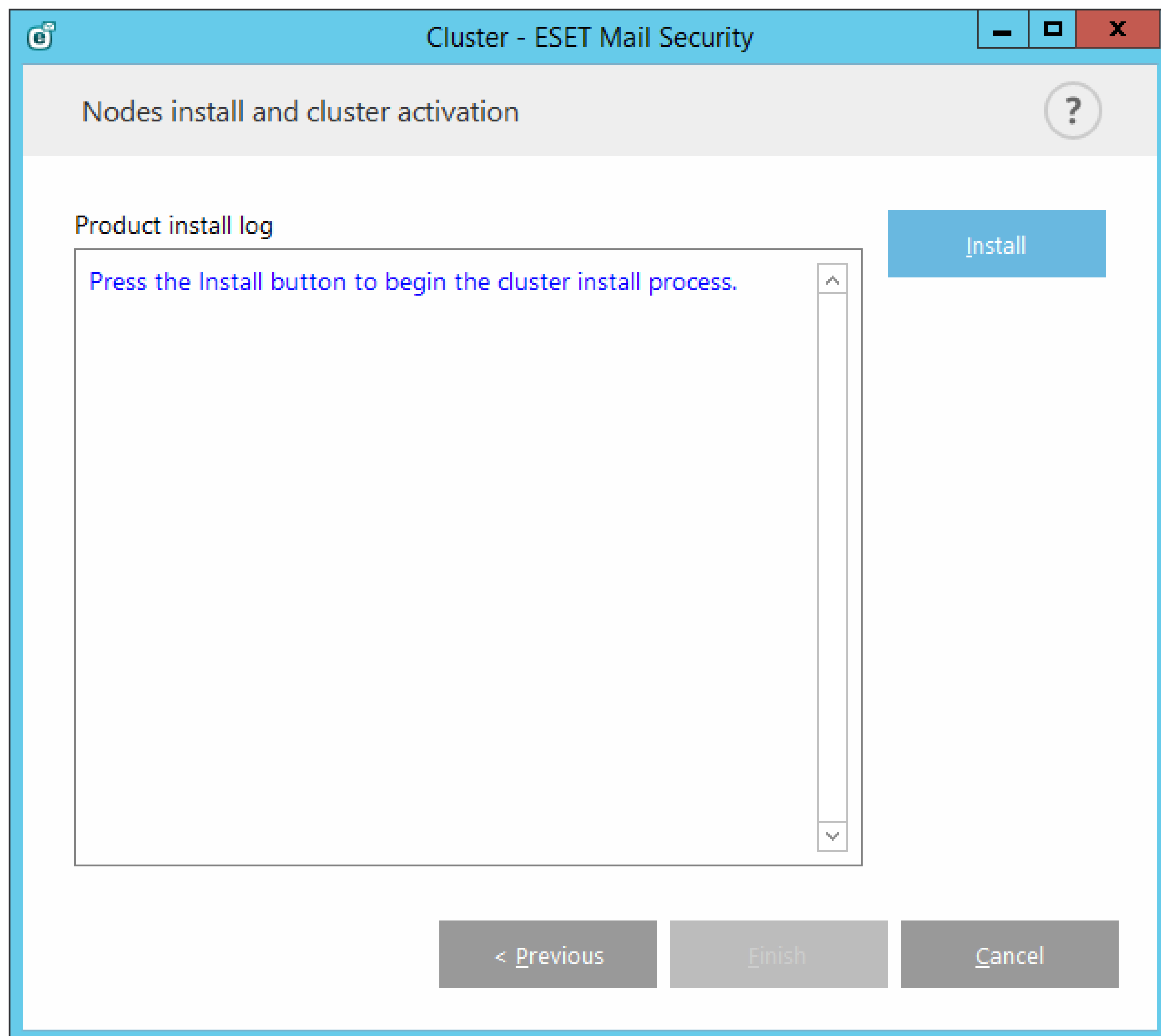


Você verá o relatório assim que a verificação de nó for concluída:



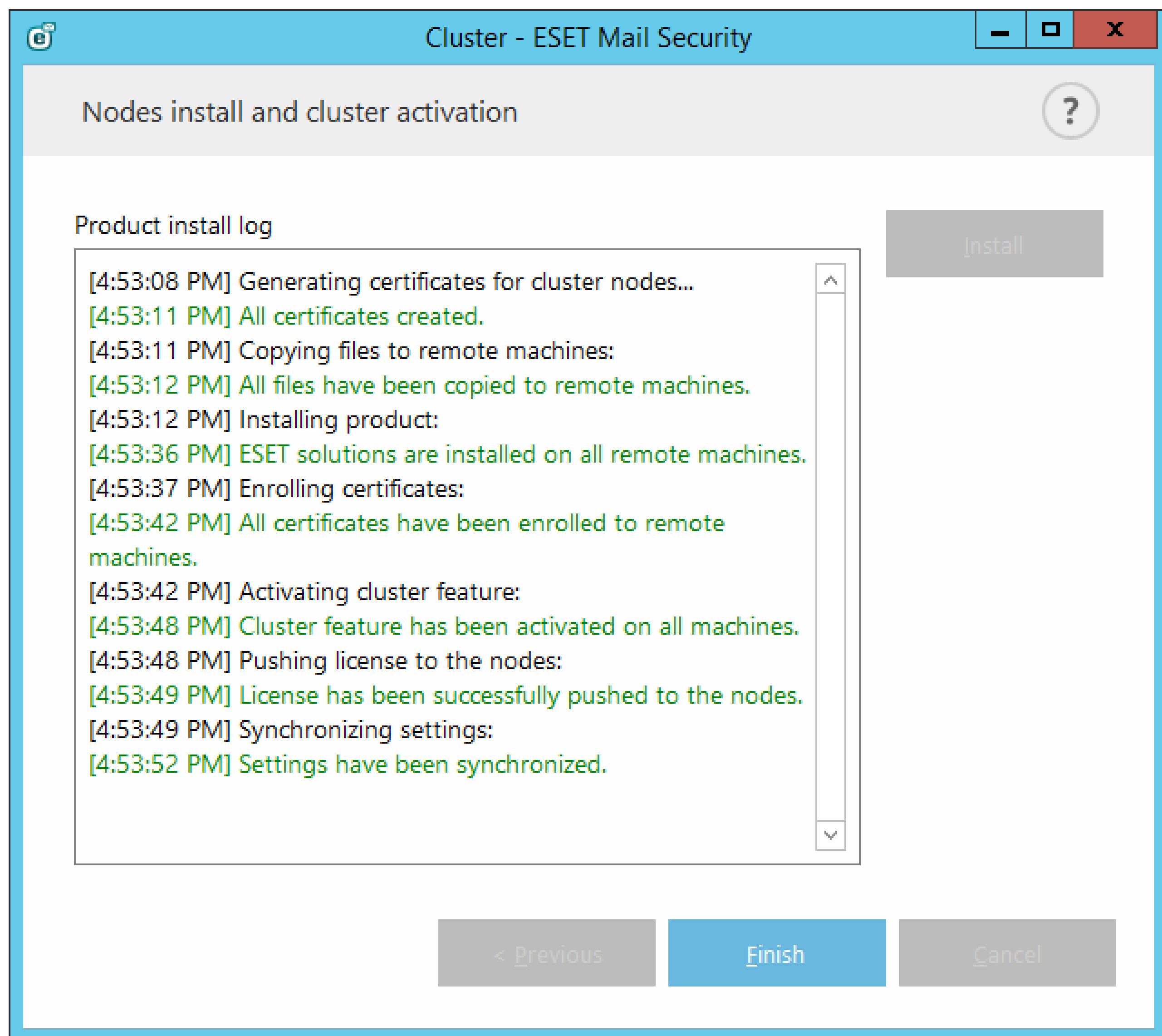
5.1.10.4 Assistente do agrupamento - página 4

Quando o produto tiver que ser instalado em uma máquina remota durante a inicialização do Agrupamento ESET, o pacote do instalador verifica o diretório %ProgramData%\ESET\<Produt_name>\Instalador em busca da presença do instalador. Se o pacote instalador não for encontrado aqui, o usuário é solicitado a localizar um pacote.



OBSERVAÇÃO: Ao tentar usar a instalação remota automática para um nó de uma plataforma diferente (32-bit vs 64-bit) isto será detectado e uma instalação manual será recomendada para tal nó.

OBSERVAÇÃO: Se você tiver uma versão mais antiga do ESET Mail Security já instalada em alguns nós, o ESET Mail Security precisa ser reinstalado com uma versão mais recente nessas máquinas antes de criar o agrupamento. Isso pode causar uma reinicialização automática de tais máquinas. Você será avisado caso este seja o caso.


Cluster - ESET Mail Security
Nodes install and cluster activation
Product install log
Install
[4:53:08 PM] Generating certificates for cluster nodes...
[4:53:11 PM] All certificates created.
[4:53:11 PM] Copying files to remote machines:
[4:53:12 PM] All files have been copied to remote machines.
[4:53:12 PM] Installing product:
[4:53:36 PM] ESET solutions are installed on all remote machines.
[4:53:37 PM] Enrolling certificates:
[4:53:42 PM] All certificates have been enrolled to remote machines.
[4:53:42 PM] Activating cluster feature:
[4:53:48 PM] Cluster feature has been activated on all machines.
[4:53:48 PM] Pushing license to the nodes:
[4:53:49 PM] License has been successfully pushed to the nodes.
[4:53:49 PM] Synchronizing settings:
[4:53:52 PM] Settings have been synchronized.
< Previous
Finish
Cancel

Assim que o Agrupamento ESET tiver sido configurado corretamente, ele vai aparecer na página **Configuração** > **Servidor** como ativado.

Também é possível verificar seu status atual na página de status de Agrupamento (**Ferramentas** > **Agrupamento**).

Importar certificados...

- Navegue para a pasta que contém os certificados (gerados durante o uso do Assistente do agrupamento).
- Selecione o arquivo de certificado e clique em **Abrir**.

5.2 Computador

O módulo **Computador** pode ser encontrado em **Configuração** > **Computador**. Ele exibe uma visão geral dos módulos de proteção descritos no capítulo anterior. Nesta seção, as seguintes configurações estão disponíveis:

- Proteção em tempo real do sistema de arquivos
- Rastreamento sob demanda do computador
- Rastreamento em estado ocioso
- Rastreamento na inicialização
- Mídia removível
- Proteção de documentos
- HIPS

As **opções do rastreamento** para todos os módulos de proteção (por exemplo, Proteção em tempo real do sistema de arquivos, Proteção do acesso à web, etc.) permitem que você ative ou desative a detecção do seguinte:

- Os aplicativos potencialmente indesejados (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo.
  Leia mais sobre esses tipos de aplicativos no glossário.
- Aplicativos potencialmente inseguros refere-se a software comercial legítimo que tenha o potencial de ser usado indevidamente para fins maliciosos. Exemplos de aplicativos potencialmente inseguros incluem ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.

Leia mais sobre esses tipos de aplicativos no glossário.

- **Aplicativos potencialmente suspeitos** incluem programas compactados com empacotadores ou protetores. Esses tipos de protetores são frequentemente explorados por autores de malware para impedir a detecção.

A **tecnologia Anti-Stealth** é um sistema sofisticado que detecta programas nocivos, como os rootkits, que podem se auto ocultar do sistema operacional, fazendo com que seja impossível detectá-los usando técnicas comuns de testes.

Exclusões de processos permitem que você exclua processos específicos. Por exemplo, processos da solução de backup, todas as operações de arquivo que podem ser atribuídas a esses processos excluídos são ignoradas e consideradas seguras, minimizando a interferência com o processo de backup.

As exclusões permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exclusões somente quando for absolutamente necessário, para garantir que todos os objetos sejam rastreados contra ameaças. Há situações em que você pode precisar excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação. Para instruções sobre como excluir um objeto do rastreamento, consulte Exclusões.

5.2.1 Uma infiltração foi detectada

As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como páginas da web, pastas compartilhadas, via email ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Comportamento padrão

Como um exemplo geral de como as infiltrações são tratadas pelo ESET Mail Security, as infiltrações podem ser detectadas usando:

- Proteção em tempo real do sistema de arquivos
- Proteção do acesso à Web
- Proteção do cliente de email
- Rastreamento sob demanda do computador

Cada um usa o nível de limpeza padrão e tentará limpar o arquivo e movê-lo para a Quarentena ou encerrar a conexão. Uma janela de notificação é exibida na área de notificação, no canto inferior direito da tela. Para obter mais informações sobre níveis de limpeza e de comportamento, consulte Limpeza.

Limpeza e exclusão

Se não houver uma ação predefinida a ser adotada para a Proteção em tempo real do sistema de arquivos, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não se recomenda selecionar **Nenhuma ação**, pois os arquivos infectados não serão limpos. A exceção a isso é quando você tem certeza de que um arquivo é inofensivo e foi detectado por engano.

Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo para o seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso por um processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

Várias ameaças

Se quaisquer arquivos infectados não foram limpos durante um rastreamento de computador (ou o nível de limpeza estava configurado como **Sem limpeza**), será exibida uma janela de alerta solicitando a você que selecione as ações adequadas para esses arquivos. Selecione ações para os arquivos (as ações são definidas individualmente para cada arquivo na lista) e clique em **Fim**.

Exclusão de arquivos em arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com Limpeza rígida, com esse tipo de limpeza ativado um arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.
Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET Mail Security e clique em Rastreamento do computador
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte Rastreamento do computador)
- Após a conclusão do rastreamento, revise o relatório para obter informações como o número de arquivos rastreados, infectados e limpos

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

5.2.2 Exclusões de processos

Este recurso permite que você exclua os processos de aplicativos do Rastreamento de antivírus no acesso. Estas exclusões ajudam a minimizar o risco de potenciais conflitos e melhoram o desempenho de aplicativos excluídos, que por sua vez causam um efeito positivo no desempenho global do sistema operacional.

Quando um processo é excluído, seu arquivo executável não é monitorado. A atividade de processo excluídos não é monitorada pelo ESET Mail Security e nenhuma verificação é executada em quaisquer operações de arquivos realizadas pelo processo.

Use **Adicionar**, **Editar** e **Remover** para gerenciar as exclusões de processos.

OBSERVAÇÃO: Exclusões do processo são exclusões apenas do Rastreamento de antivírus no acesso. Por exemplo, a Proteção do acesso à Web não leva em conta esta exclusão, então se você excluir o arquivo executável do seu navegador da web, arquivos baixados ainda serão rastreados. Assim, uma infiltração ainda pode ser detectada. Esse cenário é apenas um exemplo, e não recomendamos criar exclusões para navegadores web.

OBSERVAÇÃO: HIPS está envolvido na avaliação de processos excluídos, portanto recomendamos que você teste os processos recém-excluídos com HIPS ativado (ou desativado, se você tiver problemas). Desativar HIPS não vai afetar exclusões de processo. Se HIPS estiver desativado, a identificação de processos excluídos é baseada apenas no caminho.

5.2.3 Exclusões automáticas

Os desenvolvedores de aplicativos de servidor e sistemas operacionais recomendam excluir conjuntos de arquivos e pastas críticos de trabalho do rastreamento do antivírus para a maioria de seus produtos. Os rastreamentos de antivírus podem ter uma influência negativa no desempenho de um servidor, levar a conflitos e até impedir que alguns aplicativos sejam executados no servidor. As exclusões ajudam a reduzir o risco de possíveis conflitos e aumentam o desempenho geral do servidor ao executar o software antivírus.

o ESET Mail Security identifica aplicativos críticos de servidor e arquivos do sistema operacional do servidor e os adiciona automaticamente à lista de Exclusões. Você pode ver uma lista de aplicativos do servidor detectados em **Exclusões automáticas para gerar** para o qual exclusões são criadas. Por padrão, todas as exclusões automáticas estão ativadas. Você pode desativar/ativar cada aplicativo do servidor clicando na chave, com o seguinte resultado:

1. Se uma exclusão de aplicativo/sistema operacional continuar ativada, qualquer um de seus arquivos e pastas críticos serão adicionados na lista de arquivos excluídos do rastreamento (**Configuração avançada** > > **Básico** > **Exclusões** > **Editar**). Sempre que o servidor for reiniciado, o sistema realiza uma verificação automática das exclusões e restaura quaisquer exclusões que possam ter sido excluídas da lista. Esta é a configuração recomendada se quiser garantir que as Exclusões automáticas recomendadas sejam sempre aplicadas.

2. Se um usuário desativar uma exclusão de aplicativo/sistema operacional, seus arquivos e pastas críticos permanecerão na lista de arquivos excluídos do rastreamento (**Configuração avançada** > > **Básico** > **Exclusões**

> **Editar**). No entanto, eles não serão verificados ou renovados automaticamente na lista **Exclusões** sempre que o servidor for reiniciado (veja o ponto 1 acima). Recomendamos esta configuração para usuários avançados, que desejam remover ou alterar algumas exclusões padrão. Se quiser remover as exclusões da lista sem reiniciar o servidor, você precisará removê-las manualmente da lista (**Configuração avançada** > > **Básico** > **Exclusões** > **Editar**).

Uma exclusão definida pelo usuário e inserida manualmente (em **Configuração avançada** > > **Básico** > **Exclusões** > **Editar**) não será afetada pelas configurações descritas anteriormente.

As Exclusões automáticas de aplicativos/sistemas operacionais do servidor são selecionadas com base nas recomendações da Microsoft. Para obter detalhes, consulte os seguintes artigos da Base de conhecimento Microsoft:

- Recomendações de rastreamento de vírus para computadores corporativos operando versões compatíveis do Windows
- Recomendações para solução de problemas em um computador Exchange Server com software antivírus instalado
- Rastreamento de antivírus no nível de arquivo no Exchange 2007
- Software Antivírus no Sistema Operacional em Servidores Exchange

5.2.4 Cache local compartilhado

O cache local compartilhado melhorará o desempenho em ambientes virtualizados ao eliminar o rastreamento duplicado na rede. Isso garante que cada arquivo seja rastreado somente uma vez e armazenado no cache compartilhado. Ative a opção **Opção de cache** para salvar informações sobre rastreamentos de arquivos e pastas em sua rede no cache local. Se você realizar um novo rastreamento, o ESET Mail Security verificará se há arquivos rastreados no cache. Se os arquivos corresponderem, eles serão excluídos do rastreamento.

A configuração de **Servidor de cache** contém o seguinte**:**

- **Nome do host** - Nome ou endereço IP do computador no qual o cache está localizado.
- **Porta** - Número de porta usado para comunicação (mesmo que foi definido no Cache local compartilhado).
- **Senha** - Especifique a senha do Cache local compartilhado, se necessário.

5.2.5 Desempenho

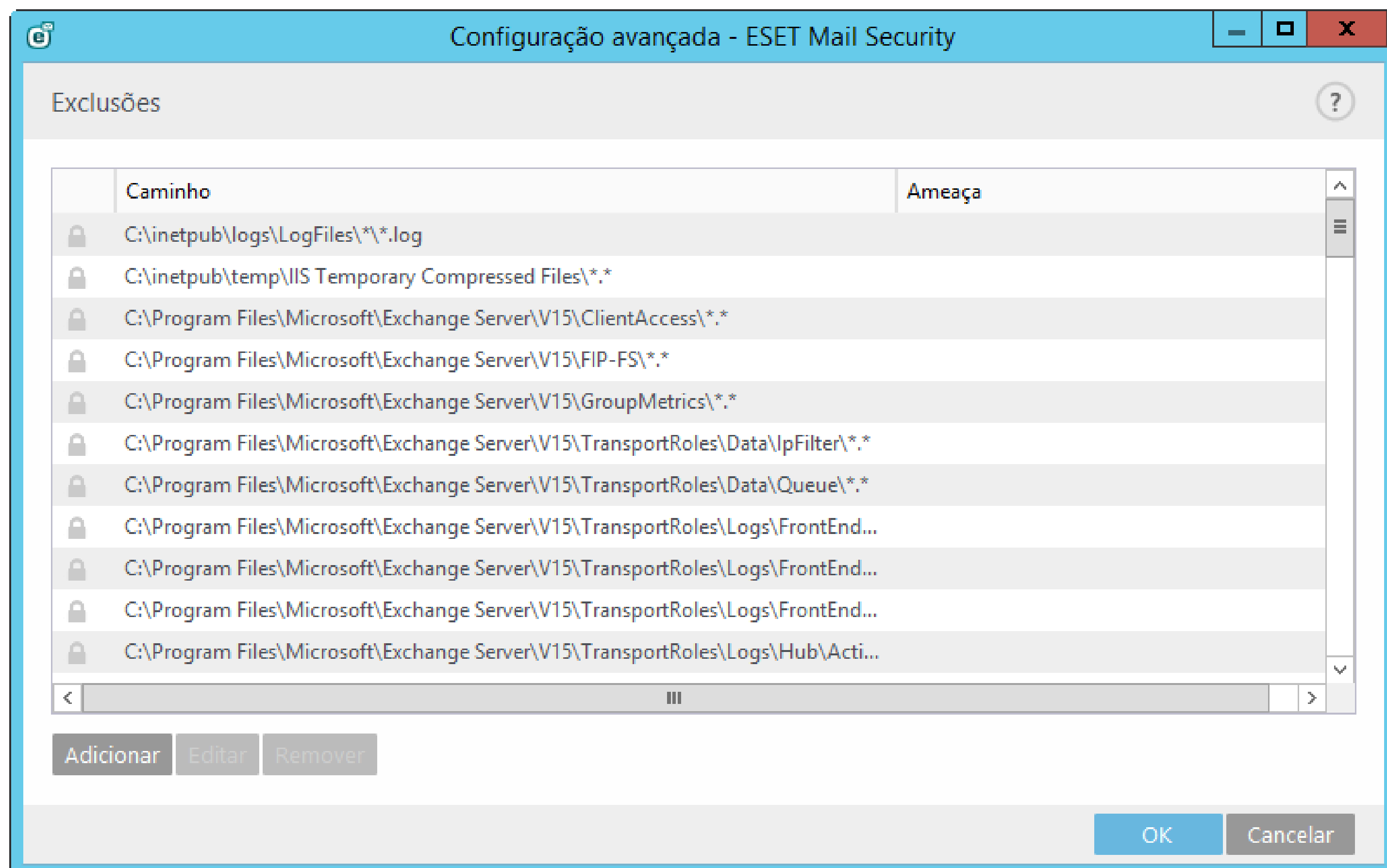
Você pode definir um número de mecanismos de rastreamento ThreatSense independentes usados pela proteção antivírus e antispyware em um momento.

Se não existirem outras restrições, recomendamos que você aumente o número de mecanismos de rastreamento do ThreatSense de acordo com esta fórmula: *número de mecanismos de rastreamento ThreatSense = (número de CPUs físicas x 2) + 1*.

i **OBSERVAÇÃO**: O valor aceitável é 1 a 20, portanto o número máximo de mecanismos de rastreamento do ThreatSense que você pode usar é 20.

5.2.6 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.



Por padrão, a proteção em tempo real do sistema de arquivos é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outra proteção em tempo real), a proteção em tempo real pode ser desativada desmarcando **Iniciar proteção em tempo real do sistema de arquivos automaticamente** em Configuração avançada, em **Proteção em tempo real do sistema de arquivos** > **Básico**.

- **Mídia a ser rastreada**

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças:

Unidades locais - Controla todas as unidades de disco rígido do sistema.
Mídia removível - Controla CD/DVDs, armazenamento USB, dispositivos Bluetooth, etc.
Unidades de rede - Rastreia todas as unidades mapeadas.

Recomendamos que você use as configurações padrão e as modifique somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

- **Rastreamento ativado**

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador:

- **Abertura de arquivo** - Ativa ou desativa o rastreamento quando arquivos estiverem abertos.
- **Criação de arquivo** - Ativa ou desativa o rastreamento quando arquivos forem criados.
- **Execução de arquivo** - Ativa ou desativa o rastreamento quando arquivos forem executados.
- **Acesso à mídia removível** - Ativa ou desativa o rastreamento disparado ao acessar mídia removível em particular com espaço de armazenamento.
- **Desligar computador** - Ativa ou desativa o rastreamento acionado por desligar o computador.

A proteção em tempo real do sistema de arquivos verifica todos os tipos de mídia e é acionada por vários eventos do sistema, tais como o acesso a um arquivo. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Parâmetros do ThreatSense), a proteção em tempo real do sistema de arquivos pode ser configurada para tratar arquivos recém-criados de forma diferente dos arquivos existentes. Por exemplo, é possível configurar a Proteção em tempo real do sistema de arquivos para monitorar mais de perto os arquivos recém-criados.

Para garantir o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é controlado usando a **Otimização inteligente**. Se a Otimização inteligente estiver desativada, todos os arquivos serão rastreados sempre que forem acessados. Para modificar essa configuração, pressione **F5** para abrir a Configuração avançada e expanda **Antivírus** > **Proteção em tempo real do sistema de arquivos**. Clique em **Parâmetros do ThreatSense**> **Outro** e marque ou desmarque **Ativar otimização inteligente**.

5.2.6.1 Exclusões

Não deve ser confundido com **Extensões excluídas**

As exclusões permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exclusões somente quando for absolutamente necessário, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Há situações em que você pode precisar excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação (por exemplo, software de backup).

Para excluir um objeto do rastreamento:

Clique em **Adicionar** edigite o caminho para um objeto ou selecione-o na estrutura em árvore.
Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres.

Exemplos

- Se você desejar excluir todos os arquivos em uma pasta, digite o caminho para a pasta e use a máscara “*.*”.
- Para excluir a unidade por completo, incluindo todos os arquivos e subpastas, use a máscara "D:*".
- Se você desejar excluir somente arquivos doc, use a máscara “*.doc”.
- Se o nome de um arquivo executável tiver um determinado número de caracteres (e os caracteres variarem) e você souber somente o primeiro com certeza (digamos, “D”), use o seguinte formato: "D????.exe". Os sinais de interrogação substituem os caracteres em falta (desconhecidos).

i **OBSERVAÇÃO:** uma ameaça em um arquivo não será detectada pelo módulo de proteção em tempo real do sistema de arquivos ou módulo de rastreamento do computador se um arquivo atender aos critérios para exclusão do rastreamento.

Colunas

Caminho - caminho para arquivos e pastas excluídos.
Ameaça - se houver um nome de uma ameaça exibido ao lado de um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça. Se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus. Esse tipo de exclusão pode ser utilizado apenas para determinados tipos de infiltrações e pode ser criado na janela de alerta de ameaças que informa a infiltração (clique em **Mostrar opções avançadas** e selecione **Excluir da detecção**) ou clicando em **Configuração** > **Quarentena**, clicando com o botão direito do mouse no arquivo em quarentena e selecionando **Restaurar e excluir da detecção** no menu de contexto.

Elementos de controle

Adicionar - exclui objetos da detecção.
Editar - permite que você edite as entradas selecionadas.
Remover - remove as entradas selecionadas.

5.2.6.1.1 Adicionar ou editar exclusão

Essa janela de diálogo permite adicionar ou editar exclusões. Isso pode ser feito de duas formas:

- digitando o caminho para um objeto a ser excluído
- selecionando-o na estrutura em árvore (clique em **...** no final do campo de texto para procurar)

Se você estiver usando o primeiro método, podem ser usados os caracteres curinga descritos na seção Formato de exclusão.

5.2.6.1.2 Formato da exclusão

Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres.

Exemplos

- Se você desejar excluir todos os arquivos em uma pasta, digite o caminho para a pasta e use a máscara “*.*”.
- Para excluir a unidade por completo, incluindo todos os arquivos e subpastas, use a máscara "D:*".
- Se você desejar excluir somente arquivos doc, use a máscara “*.doc”.
- Se o nome de um arquivo executável tiver um determinado número de caracteres (e os caracteres variarem) e você souber somente o primeiro com certeza (digamos, “D”), use o seguinte formato: "D????.exe". Os sinais de interrogação substituem os caracteres em falta (desconhecidos).

5.2.6.2 Parâmetros ThreatSense

o ThreatSense é a tecnologia que consiste em muitos métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante a propagação inicial de uma nova ameaça. Ela utiliza uma combinação de análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

as opções de configuração do motor ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique em **Configuração de parâmetro do mecanismo ThreatSense** na janela de Configuração avançada de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos
- Rastreamento em estado ocioso
- Rastreamento na inicialização
- Proteção de documentos
- Proteção do cliente de email
- Proteção do acesso à Web
- Rastreamento do computador

Os parâmetros do ThreatSense são altamente otimizados para cada módulo, e modificá-los pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar a heurística avançada no módulo de Proteção em tempo real do sistema de arquivos pode resultar em maior utilização dos recursos (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastreamento do computador.

Objetos a serem rastreados

Esta seção permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

- **Memória operacional** - Rastreia procurando ameaças que atacam a memória operacional do sistema.
- **Setores de inicialização** - Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.
- **Arquivos de email** - O programa oferece suporte às seguintes extensões: DBX (Outlook Express) e EML.
- **Arquivos compactados** - O programa oferece suporte às seguintes extensões: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e muitas outras.
- **Arquivos compactados de autoextração** - Os arquivos compactados de autoextração (SFX, Self-extracting archives) são arquivos compactados que não requerem programas especializados - arquivos compactados - para se descompactarem.
- **Empacotadores em tempo real** - Depois da execução, os empacotadores em tempo real (ao contrário dos arquivos compactados padrão) fazem a descompactação na memória. Além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FSG etc.), o rastreamento é compatível com o reconhecimento de vários tipos adicionais de empacotadores graças à emulação do código.

Opções de rastreamento

Selecione os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

- **Heurística** - Uma heurística é um algoritmo que analisa a atividade (maliciosa) dos programas. A principal vantagem dessa tecnologia é a capacidade de identificar software malicioso que não existia ou que não era conhecido pelo banco de dados de assinaturas de vírus anterior. A desvantagem é uma probabilidade (muito pequena) de alarmes falsos.
- **Heurística avançada/DNA/Assinaturas inteligentes** - A heurística avançada consiste em um algoritmo de heurística exclusivo desenvolvido pela ESET, otimizado para detecção de worms e cavalos de troia no computador e escrito em linguagens de programação de alto nível. O uso de heurística avançada aumenta muito as capacidades de detecção de ameaças de produtos ESET. As assinaturas podem detectar e identificar vírus com segurança. Usando o sistema de atualização automática, novas assinaturas são disponibilizadas em poucas horas depois da descoberta da ameaça. A desvantagem das assinaturas é que elas detectam somente os vírus que conhecem (ou suas versões levemente modificadas).

Os **aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento antes da instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- Novas janelas que você não via anteriormente (pop-ups, ads)
- Ativação e execução de processos ocultos
- Uso aumentado de recursos do sistema
- Alterações nos resultados de pesquisa
- O aplicativo comunica-se com servidores remotos

- **Aplicativos potencialmente inseguros** - Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Ela inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.
- **ESET Live Grid** - Graças à tecnologia de reputação da ESET, as informações sobre os arquivos rastreados são verificadas em relação aos dados do ESET Live Grid baseado na nuvem, a fim de melhorar a detecção e a velocidade de rastreamento.

Limpeza

As configurações de limpeza determinam o comportamento do rastreamento enquanto limpa os arquivos infectados. Há três níveis de limpeza:

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza normal - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela.. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpar um arquivo, o usuário será solicitado a selecionar o tipo de ação a ser realizada.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem infectados. No modo **Limpeza rígida**, o arquivo compactado será excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

Exclusões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Outros

Ao configurar os parâmetros do mecanismo ThreatSense para um rastreamento sob demanda do computador, as seguintes opções na seção **Outro** também estarão disponíveis:

- **Rastrear fluxos dados alternativos (ADS)** - Fluxos de dados alternativos usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.
- **Executar rastreamento em segundo plano com baixa prioridade** - Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.
- **Registrar todos os objetos** - Se essa opção estiver selecionada, o relatório mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados. Por exemplo, se uma infiltração for encontrada dentro de um arquivo compactado, o relatório também listará os arquivos limpos contidos dentro do arquivo compactado.
- **Ativar otimização inteligente** - Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de rastreamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.
- **Manter último registro de acesso** - Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Configurações do objeto

Configurações do objeto padrão

- **Tamanho máximo do objeto** - Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Essa opção apenas será alterada por usuários avançados que podem ter razões específicas para excluir objetos maiores do rastreamento. Valor padrão: *sem limite*.
- **Tempo máximo do rastreamento para objeto (s)** - Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento. Valor padrão: *sem limite*.

Configuração de rastreamento em arquivos compactados

Nível de compactação de arquivos compactados - Especifica a profundidade máxima do rastreamento de arquivos compactados. Valor padrão: *10*.

Tamanho máximo do arquivo no arquivo compactado - Essa opção permite especificar o tamanho máximo de arquivos para os arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Valor padrão: *sem limite*.

OBSERVAÇÃO: Não recomendamos alterar os valores padrão; sob circunstâncias normais, não haverá razão para modificá-los.

5.2.6.2.1 Extensões excluídas

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento.

A exclusão de arquivos será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando certas extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

Com os botões **Adicionar** e **Remover**, você pode autorizar ou proibir o rastreamento de extensões de arquivos específicas. Para adicionar uma nova extensão à lista, clique em Adicionar, digite a extensão no campo em branco e clique em OK. Quando você selecionar **Inserir valores múltiplos**, você poderá adicionar várias extensões de arquivos delimitadas por linhas, vírgulas ou ponto e vírgulas. Quando a seleção múltipla estiver ativada, extensões serão mostradas na lista. Selecione uma extensão na lista e clique em **Remover** para excluir essa extensão da lista. Se você quiser editar uma extensão selecionada, clique em **Editar**.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco representa qualquer string de caracteres e o ponto de interrogação representa qualquer símbolo.

5.2.6.2.2 Parâmetros ThreatSense adicionais

Parâmetros ThreatSense adicionais para arquivos criados e modificados recentemente - A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior do que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, também é usada a heurística avançada, que pode detectar novas ameaças antes do lançamento da atualização do banco de dados de assinatura de vírus. Além dos arquivos recém-criados, o rastreamento é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desative **Configurações padrão de rastreamento em arquivos compactados**.

Para saber mais sobre **Empacotadores em tempo real**, **Arquivos compactados de auto extração** e **Heurística avançada** consulte a configuração de parâmetros do mecanismo do ThreatSense.

Parâmetros ThreatSense adicionais para arquivos executados - Por padrão, a heurística avançada é usada quando os arquivos são executados. Quando ativada, é altamente recomendado manter a Otimização inteligente e o ESET Live Grid ativados para minimizar o impacto no desempenho do sistema.

5.2.6.2.3 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar as configurações de nível de limpeza, clique em **Parâmetros ThreatSense** na seção **Proteção em tempo real do sistema de arquivos** e clique em **Limpeza**).

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza normal - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela.. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpar um arquivo, o usuário será solicitado a selecionar o tipo de ação a ser realizada.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem infectados. No modo **Limpeza rígida**, o arquivo compactado será excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

5.2.6.2.4 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real do sistema de arquivos é o componente mais essencial para a manutenção de um sistema seguro. Seja sempre cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos.

Após a instalação do ESET Mail Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique em ao lado de cada guia na janela (**Configuração avançada** > > **Proteção em tempo real do sistema de arquivos**).

5.2.6.2.5 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.com. Este arquivo de teste é inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo está disponível para download em http://www.eicar.org/download/eicar.com

5.2.6.2.6 O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos problemas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** na janela principal do programa e clique em **Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não for ativada na inicialização do sistema, geralmente é porque **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está desativada. Para ativar essa opção, navegue até Configuração avançada (**F5**) e clique em **Computador** > **Proteção em tempo real do sistema de arquivos** > **Básica** na seção **Configuração avançada**. Certifique-se de que **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está ativado.

Se a proteção em tempo real não detectar nem limpar infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema antes da instalação da ESET.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e estiver ativado **Iniciar automaticamente proteção em tempo real do sistema de arquivos**), isto pode ser devido a conflitos com outros programas. Para ajuda na resolução deste problema, entre em contato com o Atendimento ao cliente da ESET.

5.2.6.2.7 Envio

Você pode selecionar como os arquivos e as informações estatísticas serão enviados à ESET. Selecione a opção **Através do Administrador Remoto ou diretamente para a ESET** para enviar arquivos e estatísticas por qualquer meio disponível. Selecione a opção **Através do Administrador Remoto**para enviar os arquivos e as estatísticas ao servidor da administração remota, que assegurará o envio posterior ao Laboratório de ameaças da ESET. Se **Diretamente para a ESET** estiver selecionada, todos os arquivos suspeitos e as informações estatísticas serão enviados ao laboratório de análise de vírus da ESET a partir do programa.

Quando houver arquivos com envio pendente, o botão **Enviar agora** estará ativado. Clique nesse botão para enviar arquivos e informações estatísticas imediatamente.

Selecione **Ativar registro em relatório** para criar um relatório para registrar os envios de arquivos e informações estatísticas.

5.2.6.2.8 Estatísticas

O ThreatSense.Net Early Warning System coletará informações anônimas sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir o nome da ameaça, a data e o horário em que ela foi detectada, a versão do produto de segurança da ESET, a versão do seu sistema operacional e a configuração de local. As estatísticas são normalmente enviadas aos servidores da ESET, uma ou duas vezes por dia.

A seguir há um exemplo de um pacote estatístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Quando enviar - Você pode definir o momento em que as informações estatísticas serão enviadas. Se optar por enviar **O mais breve possível**, as informações estatísticas serão enviadas imediatamente após serem criadas. Esta configuração é adequada se um conexão permanente com a Internet estiver disponível. Se a opção **Durante a atualização** estiver selecionada, todas as informações estatísticas serão enviadas em grupo durante a próxima atualização.

5.2.6.2.9 Arquivos suspeitos

A guia **Arquivos suspeitos** permite configurar a maneira como as ameaças serão enviadas ao Laboratório de ameaças da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de ameaças. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

O envio de arquivos pode ser definido para ocorrer automaticamente ou selecione a opção **Perguntar antes de enviar**, se quiser saber quais arquivos foram enviados para análise e confirmar o envio.

Se não desejar que os arquivos sejam enviados, selecione a opção **Não enviar para análise**. A seleção da opção de não envio de arquivos para análise não influencia o envio das informações estatísticas, que são definidas em sua própria configuração. (consulte a seção Estatísticas).

Quando enviar - Por padrão, a opção **O mais breve possível** fica selecionada para que os arquivos suspeitos sejam enviados ao Laboratório de ameaças da ESET. Esta é a opção recomendada se uma conexão permanente com a Internet estiver disponível e os arquivos suspeitos puderem ser enviados sem atraso. Selecione a opção **Durante a atualização** para que o upload de arquivos suspeitos seja feito para o ThreatSense.Net durante a próxima atualização.

Filtro de exclusões – O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de

arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Email de contato – Seu **Email de contato (opcional)**pode ser enviado com qualquer arquivo suspeito e pode ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

5.2.7 Rastreamento sob demanda do computador

Esta seção fornece opções para a escolha dos parâmetros do rastreamento.

Perfil selecionado - Um conjunto particular de parâmetros usados pelo rastreador sob demanda. Para criar um novo, clique em **Editar** ao lado de **Lista de perfis**.

Se você quiser rastrear somente um destino específico, você pode clicar em **Editar** ao lado de **Alvos de rastreamento** e escolha uma opção no menu suspenso ou selecionar alvos específicos da estrutura de pastas (árvore).

A janela de alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Pastas compartilhadas** - Seleciona todas as pastas compartilhadas no servidor local.
- **Nenhuma seleção** - Cancela todas as seleções.

Clique em parâmetros do ThreatSense para modificar parâmetros de rastreamento (por exemplo, métodos de detecção) para o rastreamento do computador sob demanda.

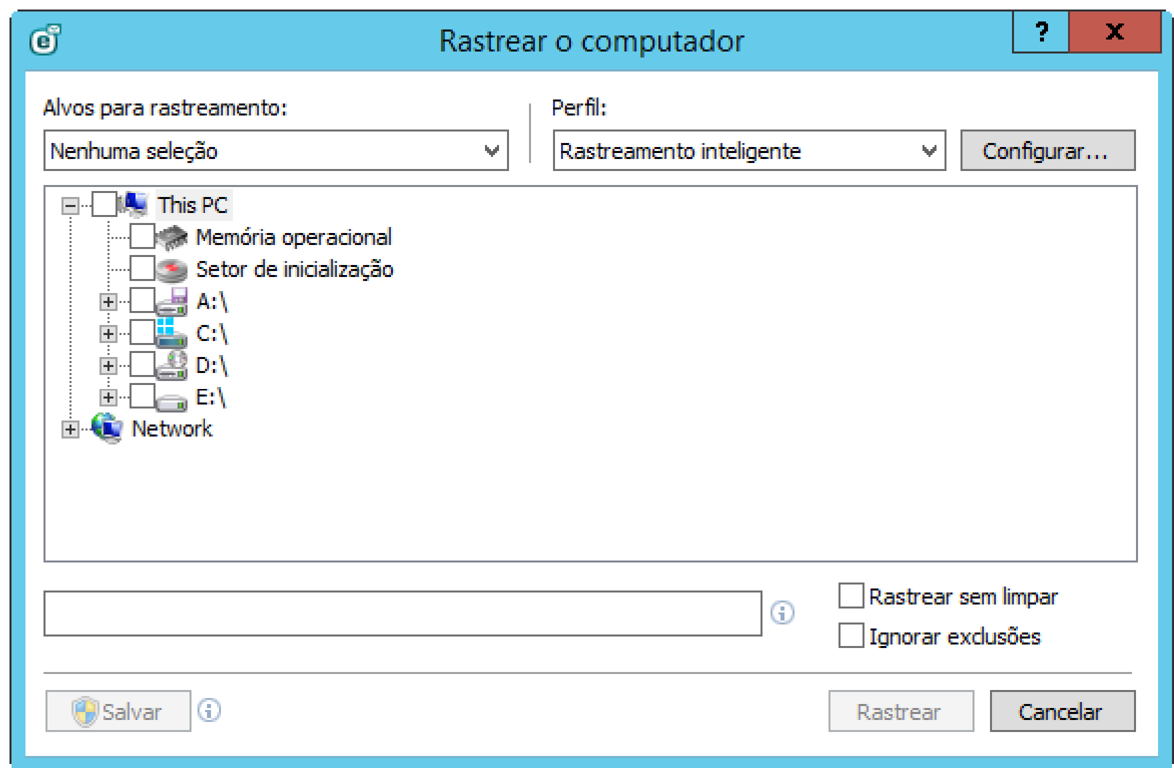
5.2.7.1 Iniciador de rastreamento personalizado

Se desejar verificar um alvo específico, você poderá usar a ferramenta Rastreamento personalizado clicando em **Rastreamento do computador** > **Rastreamento personalizado** e selecionar uma opção no menu suspenso **Destinos de rastreamento** ou selecionar alvos específicos na estrutura de pasta (em árvore).

A janela de alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Pastas compartilhadas** - Seleciona todas as pastas compartilhadas no servidor local.
- **Nenhuma seleção** - Cancela todas as seleções.

Para navegar rapidamente até um alvo de rastreamento selecionado ou para adicionar diretamente um alvo desejado (pasta ou arquivo(s)), digite-o no campo em branco embaixo da lista de pastas. Isso só é possível se nenhum alvo tiver sido selecionado na estrutura em árvore e se o menu **Alvos de rastreamento** estiver definido como **Nenhuma seleção**.



Os itens infectados não são limpos automaticamente. O rastreamento sem limpar pode ser usado para obter uma visão geral do status da proteção atual. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração** > **Parâmetros Threatsense** > **Limpeza**. As informações sobre o rastreamento serão salvas em um relatório de rastreamento.

Você pode escolher um perfil no menu suspenso **Perfil de rastreamento** para ser usado para rastreamento dos alvos escolhidos. O perfil padrão é **Rastreamento inteligente**. Há mais dois perfis de rastreamento predefinidos intitulados **Rastreamento detalhado** e **Rastreamento do menu de contexto**. Estes perfis de rastreamento usam parâmetros diferentes do motor ThreatSense. Clique em **Configuração...** para configurar em detalhes o perfil de rastreamento escolhido no menu Perfil de rastreamento. As opções disponíveis são descritas na seção **Outro** na Configuração de parâmetros do mecanismoThreatSense.

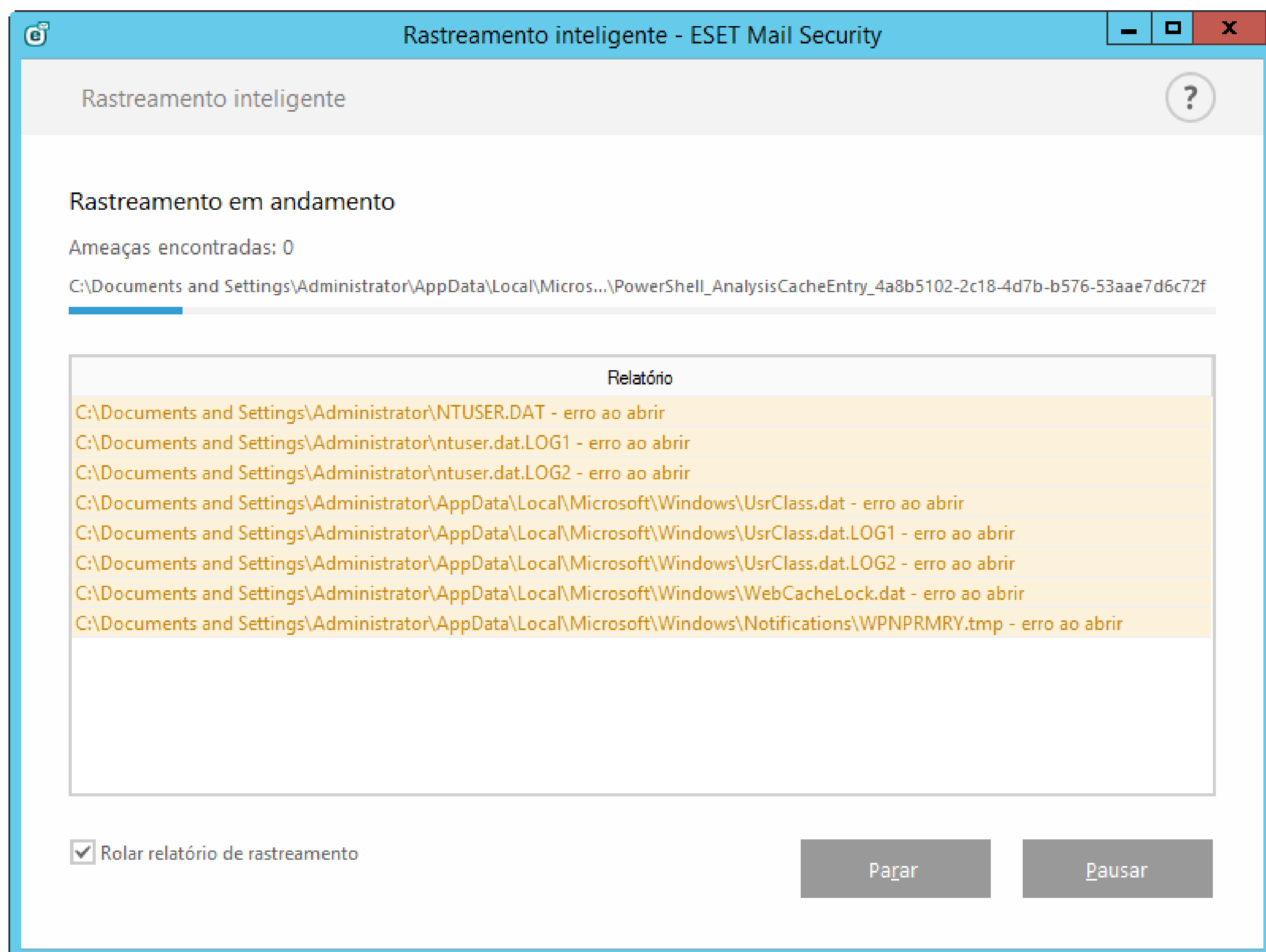
Clique em **Salvar** para salvar as alterações feitas na sua seleção de alvos, incluindo seleções feitas dentro da estrutura em árvore da pasta.

Clique em **Rastrear** para executar o rastreamento com os parâmetros personalizados definidos.

Rastrear como administrador permite que você execute o rastreamento usando a conta do administrador. Clique nessa opção se o usuário atual não tiver privilégios para acessar os arquivos apropriados para serem rastreados. Observe que esse botão não estará disponível se o usuário atual não puder acionar operações de UAC como Administrador.

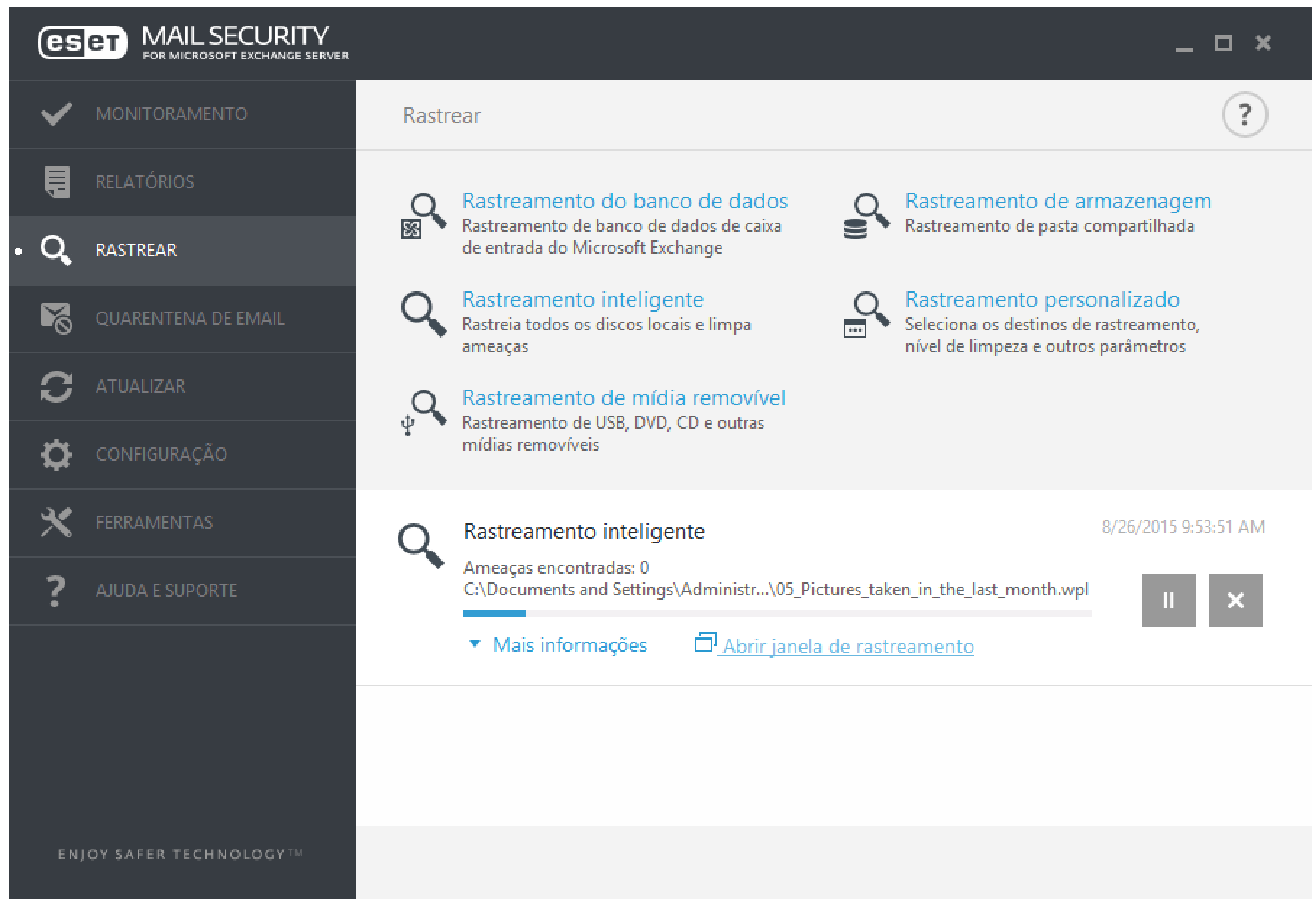
5.2.7.2 Progresso do rastreamento

A janela de progresso do rastreamento mostra o status atual do rastreamento e informações sobre a quantidade de arquivos encontrados que contêm código malicioso.



OBSERVAÇÃO: É normal que alguns arquivos, como arquivos protegidos por senha ou arquivos exclusivamente utilizados pelo sistema (geralmente *pagefile.sys* e determinados relatórios), não possam ser rastreados.

Progresso do rastreamento - A barra de progresso mostra o status de objetos já rastreados em relação aos objetos ainda aguardando para serem rastreados. O status de progresso do rastreamento é derivado do número total de objetos incluídos no rastreamento.
Destino - O nome do objeto rastreado no momento e sua localização.
Ameaças encontradas - Mostra o número total de ameaças encontradas durante um rastreamento.
Pausa - Pausa um rastreamento.
Continuar - Essa opção torna-se visível quando o progresso do rastreamento é pausado. Clique em Continuar para dar continuidade ao rastreamento.
Parar - Termina o rastreamento.
Percorrer relatório de rastreamento - Se estiver ativado, o relatório de rastreamento rolará automaticamente para baixo à medida que novas entradas forem adicionadas para que as entradas mais recentes fiquem visíveis.



5.2.7.3 Gerenciador de perfil

O gerenciador de perfil é usado em duas seções no ESET Mail Security - **Rastreamento sob demanda do computador** e **Atualizar**.

Rastreamento sob demanda do computador

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela de configuração avançada (F5) e clique em > **Rastreamento sob demanda do computador** e em **Editar** ao lado de **Lista de perfis**. O menu suspenso **Perfil selecionado** que lista os perfis de rastreamento existentes. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de

Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Digite o nome do novo perfil na janela **Gerenciador de perfil** e clique em **Adicionar**. Selecione seu novo perfil do menu suspenso **Perfil selecionado** e ajuste os parâmetros restantes para atender aos seus requisitos e clique em **OK** para salvar seu novo perfil.

Atualizar

O editor de perfil na seção de configuração da Atualização permite que os usuários criem novos perfis de atualização. Crie e use os seus próprios perfis personalizados (isto é, outros que não sejam o padrão **Meu perfil**) somente se o seu computador usar diversos modos de conexão com os servidores de atualização.

Por exemplo, um laptop que normalmente se conecta ao servidor local (Imagem) na rede local, mas faz os downloads das atualizações diretamente dos servidores de atualização da ESET quando está desconectado da rede local (em viagem de negócios, por exemplo) pode usar dois perfis: o primeiro para conectar ao servidor local; o segundo para conectar aos servidores da ESET. Quando esses perfis estiverem configurados, navegue até **Ferramentas** > **Agenda** e edite os parâmetros da tarefa de atualização. Designe um perfil como primário e outro como secundário.

Perfil selecionado - O perfil de atualização atualmente usado. Para mudar isso, escolha um perfil no menu.

Lista de perfis - Crie novos perfis de atualização ou edição.

5.2.7.4 Alvos de rastreamento

A janela de alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Pastas compartilhadas** - Seleciona todas as pastas compartilhadas no servidor local.
- **Nenhuma seleção** - Cancela todas as seleções.

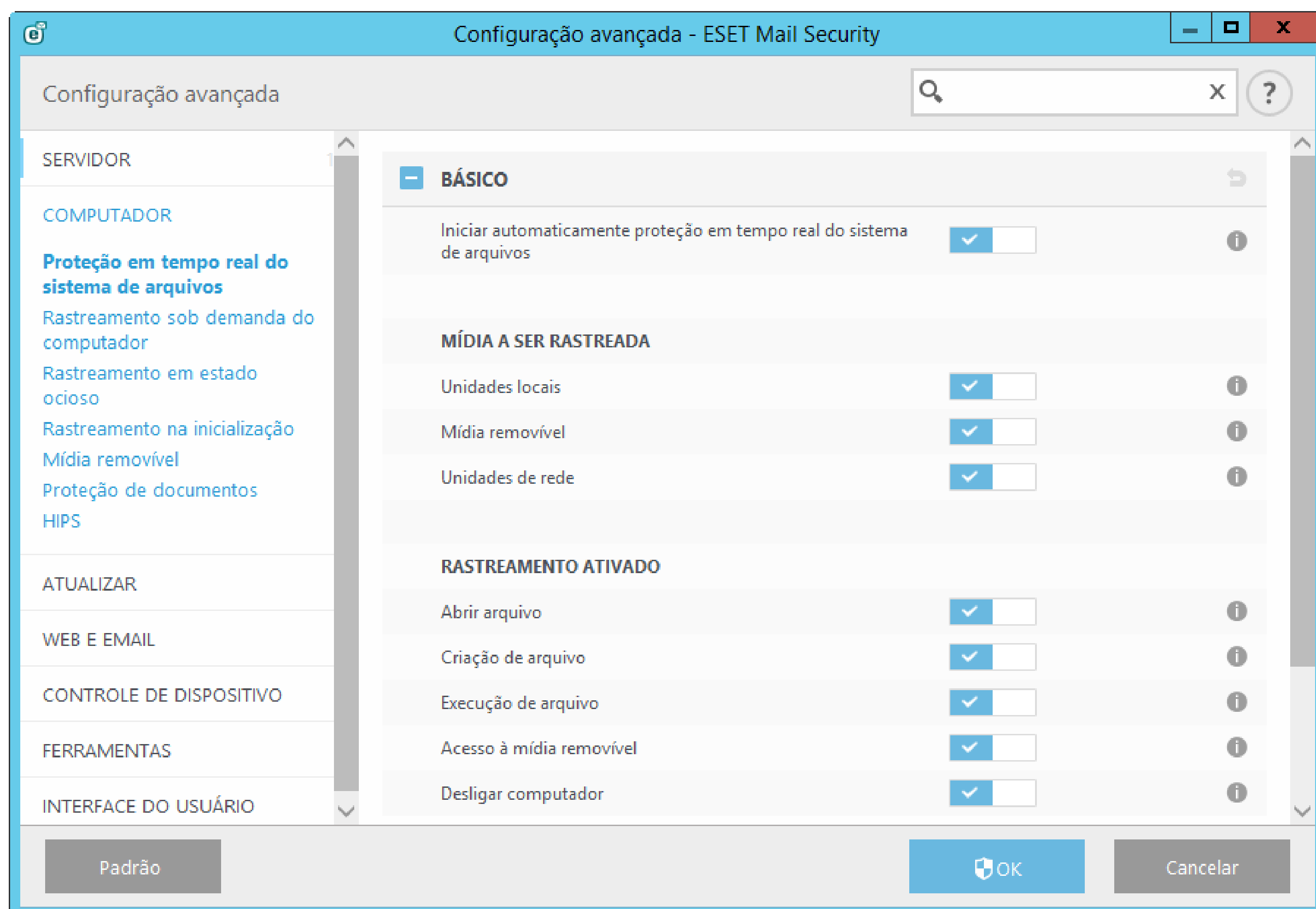
5.2.7.5 Pausar um rastreamento agendado

O rastreamento agendado pode ser adiado. Defina um valor para a opção **Interromper rastreamentos programados em (min.)** caso deseje adiar o rastreamento do computador.

5.2.8 Rastreamento em estado ocioso

Você pode ativar o rastreamento em estado ocioso em **Configuração avançada** em > **Rastreamento em estado ocioso** > **Básico**. Defina a opção ao lado de **Ativar rastreamento em estado ocioso** como Ativado para ativar esse recurso. Quando o computador estiver em estado ocioso, um rastreamento sem segundo plano do computador será realizado em todas as unidades locais.

Por padrão, o rastreamento de estado ocioso não será executado quando o computador estiver fazendo uso de bateria. Você pode substituir essa configuração marcando a caixa de seleção ao lado de **Executar mesmo se o computador estiver na bateria** na Configuração avançada.



Ative a opção **Ativar registro** na Configuração avançada para registrar uma saída de rastreamento do computador na seção Relatórios (a partir da janela principal do programa, clique em **Ferramentas** > **Relatórios** e selecione **Rastreamento do computador** a partir do menu suspenso **Relatório**).

A detecção em estado ocioso será executada quando o computador estiver em um dos seguintes estados:

- Proteção de tela
- Computador bloqueado
- Logoff de usuário

Clique em parâmetros do ThreatSense para modificar parâmetros de rastreamento (por exemplo, métodos de detecção) para o rastreamento em estado ocioso.

5.2.9 Rastreamento na inicialização

Por padrão o rastreamento automático de arquivo na inicialização será executado na inicialização do sistema e durante a atualização do banco de dados de assinatura de vírus. Esse rastreamento é controlado pelas Tarefas e configurações da agenda.

As opções de rastreamento na inicialização são parte de uma tarefa da agenda da **Rastreamento de arquivo na inicialização do sistema**. Para modificar suas configurações de rastreamento na inicialização, vá até **Ferramentas** > **Agenda**, clique em **Verificação automática de arquivos de inicialização** e então em **Editar**. Na última etapa, a janela Rastreamento automático de arquivo na inicialização será exibida (consulte o capítulo a seguir para obter mais detalhes).

Para obter mais instruções sobre o gerenciamento e a criação de tarefas da Agenda, consulte Criação de novas tarefas.

5.2.9.1 Iniciar automaticamente a verificação de arquivos

Ao criar uma tarefa agendada de Rastreamento de arquivo na inicialização do sistema, você tem várias opções para ajustar os seguintes parâmetros:

O menu suspenso **Nível de rastreamento** especifica a profundidade do rastreamento da execução de arquivos na inicialização do sistema. Os arquivos são organizados em ordem crescente de acordo com os seguintes critérios:

- **Somente os arquivos usados com mais frequência** (menos arquivos rastreados)
- **Arquivos frequentemente usados**
- **Arquivos comumente usados**
- **Arquivos raramente usados**
- **Todos os arquivos registrados** (mais arquivos rastreados)

Dois grupos específicos de **Nível de rastreamento** também estão inclusos:

- **Arquivos executados antes do logon do usuário** - Contém arquivos de locais que podem ser acessados sem que o usuário esteja conectado (inclui quase todos os locais de inicialização, tais como serviços, objetos auxiliares do navegador, notificação de Winlogon, entradas da Agenda do Windows, dlls conhecidos, etc.).
- **Arquivos executados após o logon do usuário** - Contém arquivos de locais que podem ser acessados após um usuário se conectar (inclui arquivos que são executados somente para um usuário específico, normalmente arquivos em *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

As listas de arquivos a serem rastreados estão fixas para cada grupo anteriormente.

Prioridade do rastreamento - O nível de prioridade usado para determinar quando um rastreamento iniciará:

- **Normal** - em uma carga média do sistema,
- **Baixa** - em uma carga baixa do sistema,
- **Mais baixa** - quando a carga do sistema é a menor possível,
- **Quando em espera** - a tarefa será realizada somente quando o sistema estiver em espera.

5.2.10 Mídia removível

O ESET Mail Security fornece rastreamento automático de mídia removível (CD/DVD/USB). Este módulo permite que você rastreie a mídia inserida. Isso pode ser útil se a intenção do administrador do computador for evitar que os usuários usem uma mídia removível com conteúdo não solicitado.

Ação a ser executada após inserção da mídia removível - Selecione a ação padrão que será desenvolvida quando um dispositivo de mídia removível for inserido no computador (CD/DVD/USB). Se a opção **Mostrar opções de rastreamento** for selecionada, será exibida uma notificação que lhe permite selecionar a ação desejada:

- **Não rastrear** - Nenhuma ação será executada e a janela **Novo dispositivo detectado** será fechada.
- **Rastreamento automático de dispositivo** - Um rastreamento do computador sob demanda do dispositivo de mídia removível inserido será executado.
- **Mostrar opções de rastreamento** - Abre a seção de configuração da mídia removível.

Quando uma mídia removível for inserida, a caixa de diálogo a seguir será exibida:

- **Rastrear agora** - Isto vai acionar o rastreamento da mídia removível.
- **Rastrear mais tarde** - O rastreamento da mídia removível será adiado.
- **Configuração** - Abre a Configuração avançada.
- **Sempre usar a opção selecionada** - Quando estiver selecionado, a mesma ação será executada quando uma mídia removível for inserida outra vez.

Além disso, o ESET Mail Security tem o recurso de Controle de dispositivos, que permite que você defina regras de utilização de dispositivos externos em um determinado computador. Acesse a seção Controle de dispositivos para obter mais detalhes sobre o controle de dispositivos.

5.2.11 Proteção de documentos

O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, tais como elementos do Microsoft ActiveX. A proteção de documentos fornece uma camada de proteção além da proteção em tempo real do sistema de arquivos, bem como pode ser desativada para aprimorar o desempenho em sistemas não expostos a um alto volume de documentos do Microsoft Office.

- **Integrar ao sistema** ativa o sistema de proteção. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em > **Proteção de documentos** na árvore Configuração avançada.

- Consulte Parâmetros do ThreatSense para mais informações sobre as configurações de Proteção de documentos.

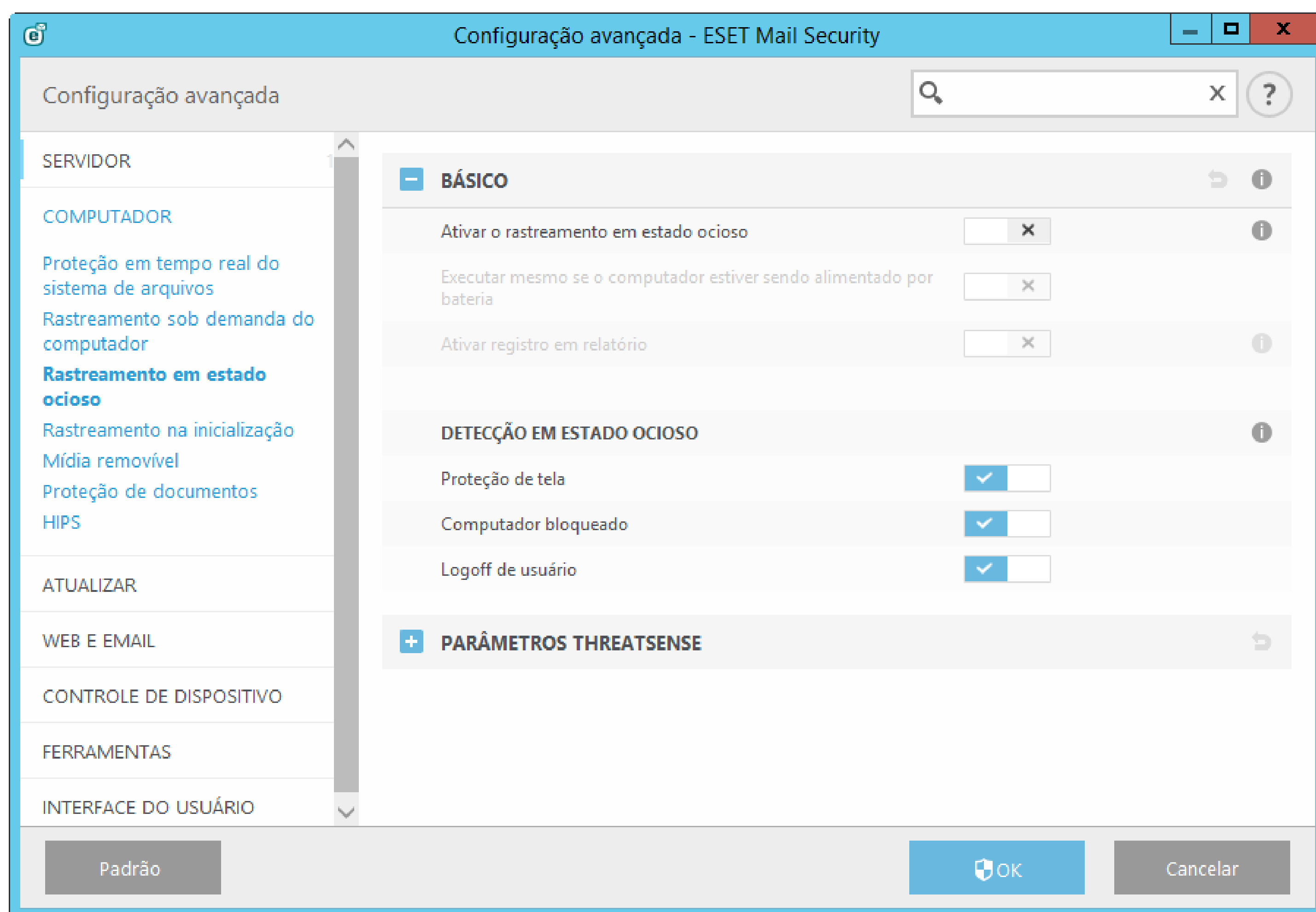
Este recurso é ativado por aplicativos que utilizam o Microsoft Antivirus API (por exemplo, Microsoft Office 2000 e superior ou Microsoft Internet Explorer 5.0 e superior).

5.2.12 HIPS

⚠ Apenas um usuário experiente deve fazer alterações nas configurações do HIPS. A configuração incorreta das configurações HIPS pode causar instabilidade no sistema.

O **Sistema de prevenção de intrusos de host** (HIPS) protege o sistema de malware ou de qualquer atividade que tentar prejudicar a segurança do computador. Ele utiliza a análise comportamental avançada em conjunto com as capacidades de detecção de filtro de rede para monitorar processos em execução, arquivos e chaves de registro. O HIPS é separado da proteção em tempo real do sistema de arquivos e não é um firewall; ele monitora somente processos em execução no sistema operacional.

As configurações do HIPS podem ser encontradas em **Configuração avançada** (F5) > > **HIPS**. O status do HIPS (ativado/desativado) é exibido na janela do programa principal do ESET Mail Security, no painel **Configuração**, à direita da seção **Computador**.



O ESET Mail Security tem uma tecnologia de *Autodefesa* incorporada que impede que o software malicioso danifique ou desabilite a proteção antivírus e antispyware. Dessa forma, você poderá ter certeza que seu sistema está protegido o tempo todo. As alterações executadas nas configurações **Ativar HIPS** e **Ativar autodefesa** entram em vigor depois que o sistema operacional Windows é reiniciado. A desativação de todo o sistema **HIPS** também exigirá uma reinicialização do computador.

O **Rastreamento de memória avançado** funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação ou criptografia. Por padrão, o rastreamento de memória avançado está ativado. Leia mais sobre esse tipo de proteção no glossário.

O **Bloqueio de exploit** é feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Por padrão, o bloqueio de exploit está ativado. Leia mais sobre esse tipo de proteção no glossário.

A filtragem pode ser executada em um de quatro modos:

- **Modo automático** - As operações são ativadas, exceto aquelas bloqueadas por regras predefinidas que protegem o sistema.
- **Modo Inteligente** - O usuário será notificado apenas sobre eventos muito suspeitos.
- **Modo interativo** - O sistema solicitará que o usuário confirme as operações.
- **Modo com base em políticas** - As operações são bloqueadas.
- **Modo de aprendizagem** - As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no Editor de regras, mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Quando selecionar o Modo de aprendizagem do menu suspenso Modo de filtragem HIPS, a configuração Modo de aprendizagem vai terminar em ficará disponível. Selecione a duração pela qual você deseja se envolver no módulo de aprendizado (a duração máxima é de 14 dias). Quando a duração especificada tiver terminado, você será solicitado a editar as regras criadas pelo HIPS enquanto ele estava no modo de aprendizagem. Você também pode escolher um modo de filtragem diferente, ou adiar a decisão e continuar usando o modo de aprendizagem.

O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com regras similares às regras usadas no firewall pessoal. Clique em **Editar** para abrir a janela de gerenciamento de regras do HIPS. Aqui é possível selecionar, criar, editar ou excluir regras. Mais detalhes sobre a criação de regras e operações HIPS podem ser encontrados no capítulo Editar regra.

Se a ação padrão para uma regra estiver definida como Perguntar, uma janela de diálogo será exibida sempre que a regra for acionada. Você pode optar por **Bloquear** ou **Permitir** a operação. Se você não definir uma ação no tempo determinado, uma nova ação será selecionada com base nas regras.

A janela da caixa de diálogo permite que você crie uma regra com base em qualquer nova ação que o HIPS detectar e então definirá as condições nas quais permitir ou bloquear essa ação. Os parâmetros exatos podem ser definidos depois de clicar em **Mostrar opções**. As regras criadas como esta são consideradas iguais às regras criadas manualmente, portanto a regra criada a partir de uma janela de diálogo pode ser menos específica que a regra que acionou a janela de diálogo. Isso significa que após a criação dessa regra, a mesma operação pode acionar a mesma janela.

Lembrar temporariamente desta ação para este processo faz com que a ação (**Permitir/Bloquear**) seja utilizada até que ocorra uma alteração de regras ou o modo de filtragem ou ocorra uma atualização do módulo do HIPS ou reinicialização do sistema. Depois de qualquer uma dessas três ações, as regras temporárias serão excluídas.

5.2.12.1 Regras HIPS

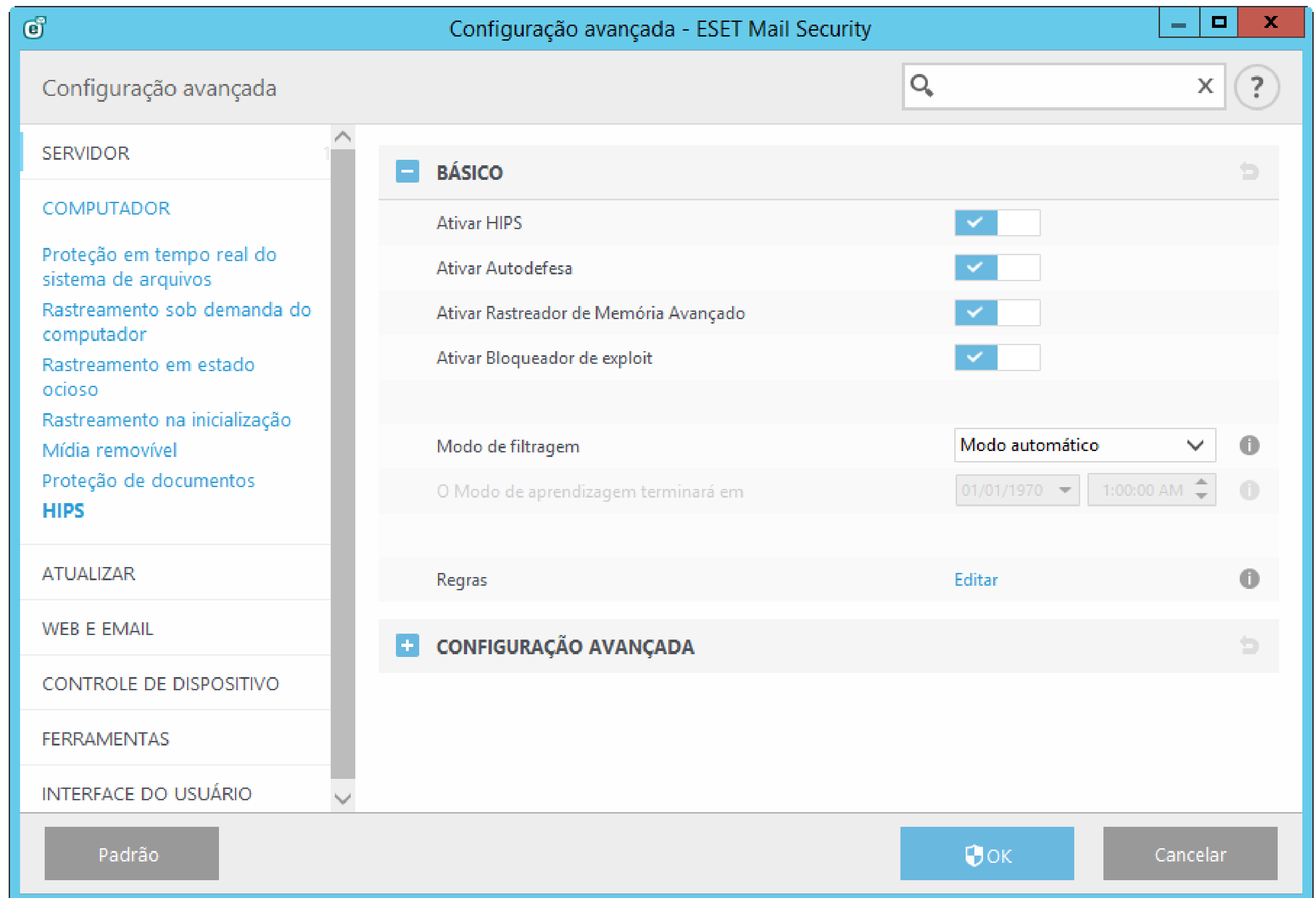
Esta janela oferece uma visão geral das regras HIPS existentes.

Colunas

Regra - Nome da regra definida pelo usuário ou definida automaticamente.
Ativado - Desative esta opção se deseja manter a regra na lista, mas não deseja usá-la.
Ação - A regra especifica uma ação - **Permitir**, **Bloquear** ou **Perguntar** - que deve ser realizada se as condições forem atendidas.
Fontes - A regra será utilizada apenas se o evento for acionado por um aplicativo(s).
Destinos - A regra será utilizada apenas se a operação estiver relacionada a um arquivo, aplicativo ou entrada de registro específico.
Relatório - Se ativar essa opção, as informações sobre esta regra serão gravadas no Relatório HIPS.
Notificar - Se um evento for acionado, uma pequena janela pop-up será exibida no canto inferior direito.

Elementos de controle

Adicionar -Cria uma nova regra.
Editar - permite que você edite as entradas selecionadas.
Remover - remove as entradas selecionadas.



5.2.12.1.1 Configurações de regra HIPS

- **Nome da regra** - Nome da regra definida pelo usuário ou definida automaticamente.
- **Ação** - A regra especifica uma ação - **Permitir**, **Bloquear** ou **Perguntar** - que deve ser realizada se as condições forem atendidas.
- **Operações afetando** - É preciso selecionar o tipo de operação para o qual a regra será aplicada. A regra será utilizada apenas para esse tipo de operação e para o destino selecionado.
- **Arquivos** - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione Arquivos específicos no menu suspenso e clique em Adicionar para adicionar novos arquivos ou pastas, ou selecione Todos os arquivos no menu suspenso para adicionar todos os aplicativos.
- **Aplicativos**- A regra será utilizada apenas se o evento for acionado por esse(s) aplicativo(s). Selecione Aplicativos específicos no menu suspenso e clique em Adicionar para adicionar novos arquivos ou pastas, ou selecione Todos os aplicativos no menu suspenso para adicionar todos os aplicativos.
- **Entradas do registro** - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione Entradas específicas no menu suspenso e clique em Adicionar para adicionar novos arquivos ou pastas, ou selecione Todas as entradas no menu suspenso para adicionar todos os aplicativos.
- **Ativado** - Desative esta chave se quiser manter a regra na lista, mas não deseja utilizá-la.
- **Relatório** - Se ativar essa opção, as informações sobre esta regra serão gravadas no Relatório HIPS.
- **Notificar usuário** - Se um evento for acionado, uma pequena janela pop-up será exibida no canto inferior direito.

A regra consiste em partes que descrevem as condições que acionam essa regra:

Aplicativos de origem - A regra será utilizada apenas se o evento for acionado por esse(s) aplicativo(s). Selecione **Aplicativos específicos** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todos os aplicativos** no menu suspenso para adicionar todos os aplicativos.

Arquivos - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione **Arquivos específicos** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todos os arquivos** no menu suspenso para adicionar todos os aplicativos.

Aplicativos - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione **Aplicativos específicos** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todos os aplicativos** no menu suspenso para adicionar todos os aplicativos.

Entradas do registro - A regra será utilizada apenas se a operação estiver relacionada a esse destino. Selecione **Entradas específicas** no menu suspenso e clique em **Adicionar** para adicionar novos arquivos ou pastas, ou selecione **Todas as entradas** no menu suspenso para adicionar todos os aplicativos.

Descrição de operações importantes:

Operações de arquivo

- **Excluir arquivo** - O aplicativo está solicitando permissão para excluir o arquivo de destino.
- **Gravar no arquivo** - O aplicativo está solicitando permissão para gravar no arquivo de destino.
- **Acesso direto ao disco** - O aplicativo está tentando ler do disco ou gravar no disco de forma não padrão, o que poderá impedir procedimentos comuns do Windows. Isso pode resultar na alteração de arquivos sem a aplicação das regras correspondentes. Essa operação poderá ser causada por um malware que está tentando impedir a detecção, um software de backup tentando realizar uma cópia exata de um disco ou um gerenciador de partição tentando reorganizar volumes do disco.
- **Instalar vínculo global** - Refere-se à chamada de função SetWindowsHookEx da biblioteca do MSDN.
- **Carregar driver** - Instalação e carregamento de drivers no sistema.

Operações de aplicativo

- **Depurar outro aplicativo** - Anexar um depurador ao processo. Ao depurar um aplicativo, muitos detalhes de seu comportamento podem ser visualizados e alterados, e seus dados podem ser acessados.
- **Interceptar eventos de outro aplicativo** - O aplicativo de origem está tentando obter eventos direcionados a um aplicativo específico (por exemplo, um keylogger está tentando capturar eventos do navegador).
- **Finalizar/suspender outro aplicativo** - Suspende, retoma ou finaliza um processo (pode ser acessado diretamente pelo Explorador de Processos ou pelo painel Processos).
- **Iniciar novo aplicativo** - Inicia novos aplicativos ou processos.
- **Alterar estado de outro aplicativo** - O aplicativo de origem está tentando gravar na memória do aplicativo de destino ou executar um código em seu nome. Este recurso pode ser útil para proteger um aplicativo essencial, configurando-o como um aplicativo de destino em uma regra e bloqueando o uso desta operação.

Operações de registro

- **Modificar configurações da inicialização** - Quaisquer alterações nas configurações que definem quais aplicativos serão executados na inicialização do Windows. Esses aplicativos podem ser encontrados, por exemplo, pesquisando pela chave Run no registro do Windows.
- **Excluir do registro** - Exclui uma chave de registro ou seu valor.
- **Renomear chave do registro** - Renomeia chaves do registro.
- **Alterar registro** - Cria novos valores de chaves de registro, alterando os valores existentes, movendo dados na árvore de banco de dados ou configurando direitos de usuário ou de grupos para as chaves do registro.

OBSERVAÇÃO: Ao informar um destino, você poderá utilizar caracteres curingas, mas com certas restrições. Em vez de uma chave específica, o símbolo * (asterisco) pode ser utilizado nos caminhos do registro. Por exemplo *HKEY_USERS*\software* pode significar *HKEY_USER\.default\software*, mas não *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** não é um caminho válido de chave de registro. Um caminho de chave de registro que contém * significa que "este caminho ou qualquer caminho em qualquer nível após esse símbolo". Esta é a única forma de usar os curingas em destinos de arquivo. Primeiro, a parte específica de um caminho será avaliada e, em seguida, o caminho após o símbolo curinga (*).

 Se você criar uma regra muito genérica, o alerta sobre este tipo de regra será exibido.

No exemplo a seguir demonstraremos como restringir o comportamento indesejado de aplicativos:

5.2.12.2 Configuração avançada

As opções a seguir são úteis para depurar e analisar o comportamento de um aplicativo:

Drivers sempre com permissão para carregar - Os drivers selecionados sempre tem permissão para carregar, independentemente do modo de filtragem configurado, a menos que explicitamente bloqueado pela regra do usuário.

Registrar todas as operações bloqueadas - Todas as operações bloqueadas serão gravadas no relatório HIPS.

Notificar quando ocorrerem alterações nos aplicativos de Inicialização - Exibe uma notificação na área de trabalho toda vez que um aplicativo for adicionado ou removido da inicialização do sistema.

Consulte nosso artigo da Base de conhecimento para obter uma versão atualizada desta página de ajuda.

5.2.12.2.1 Drivers sempre com permissão para carregar

Os drivers exibidos nesta lista sempre terão permissão para carregar, independentemente do modo de filtragem HIPS, a menos que explicitamente bloqueado pela regra do usuário.

Adicionar - Adiciona um novo driver.
Editar - Edita o caminho para um driver selecionado.
Remover - Remove um driver da lista.
Redefinir - Recarrega um conjunto de drivers do sistema.

i **OBSERVAÇÃO:** Clique em **Redefinir** se não quiser que os drivers adicionados manualmente sejam incluídos. Isso pode ser útil se você tiver vários drivers e não for possível excluí-los da lista manualmente.

5.3 Atualizar

As opções de configuração da atualização estão disponíveis na árvore **Configuração avançada** (tecla F5) em **Atualizar** > **Geral**. Esta seção especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação sendo usados para esses servidores.

Geral

O perfil de atualização usado atualmente é exibido no menu suspenso **Perfil selecionado**. Para criar um novo perfil, clique em **Editar** ao lado de **Lista de perfis**, insira seu próprio **Nome de perfil** e então clique em **Adicionar**.

Se tiver problemas com uma atualização, clique em **Limpar** para limpar o cache de atualização temporário.

Alertas de banco de dados de assinatura de vírus desatualizado

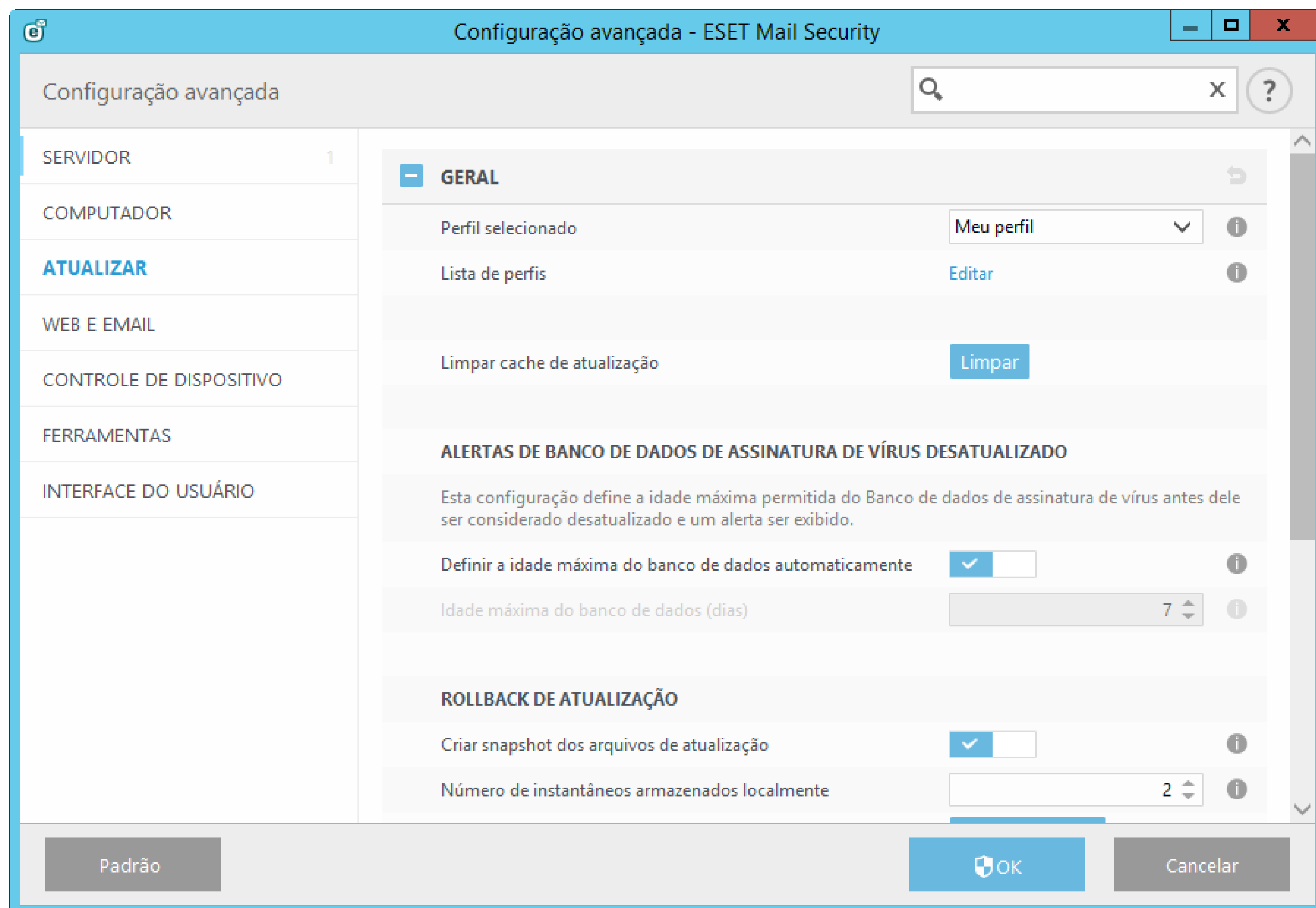
Definir a idade máxima do banco de dados automaticamente - Permite definir o tempo máximo (em dias) depois do qual o banco de dados de assinatura de vírus será relatado como desatualizado. O valor padrão é 7.

Reversão

Caso suspeite que uma nova atualização do banco de dados de vírus e/ou módulos do programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações por um período de tempo definido. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiado indefinidamente.

O ESET Mail Security registra instantâneos de módulos do programa e banco de dados de assinatura de vírus para uso com o recurso de *reversão*. Para criar instantâneos do banco de dados de vírus, deixe a caixa de seleção **Criar instantâneos dos arquivos de atualização** marcada. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do banco de dados de vírus anterior armazenado.

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Geral**), você terá que selecionar um intervalo de tempo no menu suspenso que represente o período de tempo que o banco de dados de assinatura de vírus e as atualizações do módulo do programa serão pausadas.



Para que o download das atualizações seja feito de forma adequada, é fundamental preencher corretamente todos os parâmetros de atualização. Se você usar um firewall, certifique-se de que o programa da ESET tem permissão para comunicar com a Internet (por exemplo, comunicação HTTP).

Por padrão, o **Tipo de atualização** (localizado em **Básico**) é definido como **Atualização regular** para garantir que os arquivos de atualização são obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede.

Básico

Desativar exibir notificação sobre atualização bem-sucedida - Desativa a notificação da bandeja do sistema no canto inferior direito da tela. A seleção dessa opção será útil se um aplicativo ou jogo de tela inteira estiver em execução. Lembre-se de que o Modo de apresentação desativará todas as notificações.

Por padrão, o menu **Servidor de atualização** está definido como SELEÇÃO AUTOMÁTICA. O servidor de atualização é o local onde as atualizações são armazenadas. Se você usar um servidor da ESET, recomendamos que você deixe a opção padrão selecionada. Se você estava usando um servidor de atualização personalizado e quer voltar para o padrão, digite **AUTOSELECT**. O ESET Mail Security irá selecionar automaticamente os servidores de atualização ESET.

Ao usar um servidor HTTP local - também conhecido como Imagem - o servidor de atualização deve ser definido da seguinte forma:
http://nome_computador_ou_seu_endereço_IP:2221

Ao usar um servidor HTTP local com SSL - o servidor de atualização deve ser definido da seguinte forma:
https://nome_computador_ou_seu_endereço_IP:2221

Ao usar uma pasta compartilhada local - o servidor de atualização deve ser definido da seguinte forma:
\\computer_name_or_its_IP_address\shared_folder

Atualização através da Imagem

A autenticação dos servidores de atualização é baseada no **Chave de licença** gerada e enviada ao usuário após a compra. Ao usar um servidor de imagem local, você pode definir credenciais para clientes para conexão no servidor de imagem antes do recebimento de atualizações. Por padrão, não é necessário verificação e os campos **Usuário** e **Senha** são deixados em branco.

5.3.1 Atualização de reversão

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Perfil**), você terá que selecionar um intervalo de tempo no menu suspenso que represente o período de tempo que o banco de dados de assinatura de vírus e as atualizações do módulo do programa serão pausadas.

Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. Pois isso representa um risco de segurança em potencial, não recomendamos a seleção desta opção.

A versão do banco de dados de assinatura de vírus é desatualizada para a versão mais antiga disponível e armazenada como um instantâneo no sistema de arquivos do computador local.

Exemplo: Permita que o número 10646 seja a versão mais atual do banco de dados de assinatura de vírus. 10645 e 10643 são armazenados como instantâneos do banco de dados de assinatura de vírus. Observe que 10644 não está disponível porque, por exemplo, o computador foi desligado e uma atualização mais recente foi disponibilizada antes de a 10644 ser baixada. Se você inseriu 2 (dois) no campo **Número de instantâneos armazenados localmente** e clicou em **Reverter**, o banco de dados de assinatura de vírus (incluindo módulos do programa) será restaurado para a versão número 10643. Este processo pode demorar algum tempo. Verifique se a versão do banco de dados de assinatura de vírus foi desatualizada na janela principal do programa do ESET Mail Security na seção Atualizar.

5.3.2 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa. O programa permite que você pré-defina seu comportamento quando uma nova atualização de componentes está disponível.

As atualizações de componentes do programa oferecem novos recursos ou fazem alterações nos recursos já existentes de versões anteriores. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador. Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Perguntar antes de fazer download dos componentes do programa** - Opção padrão. Você será solicitado a confirmar ou recusar as atualizações de componentes do programa quando elas estiverem disponíveis.
- **Sempre atualizar componentes do programa** - As atualizações de componentes do programa serão obtidas por download e instaladas automaticamente. Lembre-se de que pode ser necessário reiniciar o computador.
- **Nunca atualizar componentes do programa** - As atualizações de componentes do programa não serão realizadas. Esta opção é adequada para instalações de servidor, pois os servidores podem geralmente ser reiniciados somente quando estiverem em manutenção.

i **OBSERVAÇÃO:** A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

Se a opção **Perguntar antes de fazer download da atualização** estiver ativa, uma notificação será exibida quando uma nova atualização estiver disponível.

Se o tamanho do arquivo de atualização for maior que o valor especificado no campo **Perguntar se um arquivo de atualização for maior que (KB)**, o programa exibirá uma notificação.

5.3.3 Proxy HTTP

Para acessar as opções de configuração do servidor proxy de determinado perfil de atualização, clique em **Atualizar** na árvore **Configuração avançada** (F5) e clique em **Proxy HTTP**. Clique no menu suspenso **Modo proxy** e selecione uma das três opções a seguir:

- Não usar servidor proxy
- Conexão através de um servidor proxy
- Usar configurações globais de servidor proxy

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Ferramentas** > **Servidor proxy** da árvore Configuração avançada.

Selecione **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET Mail Security.

A opção **Conexão através de um servidor proxy** deve ser selecionada se:

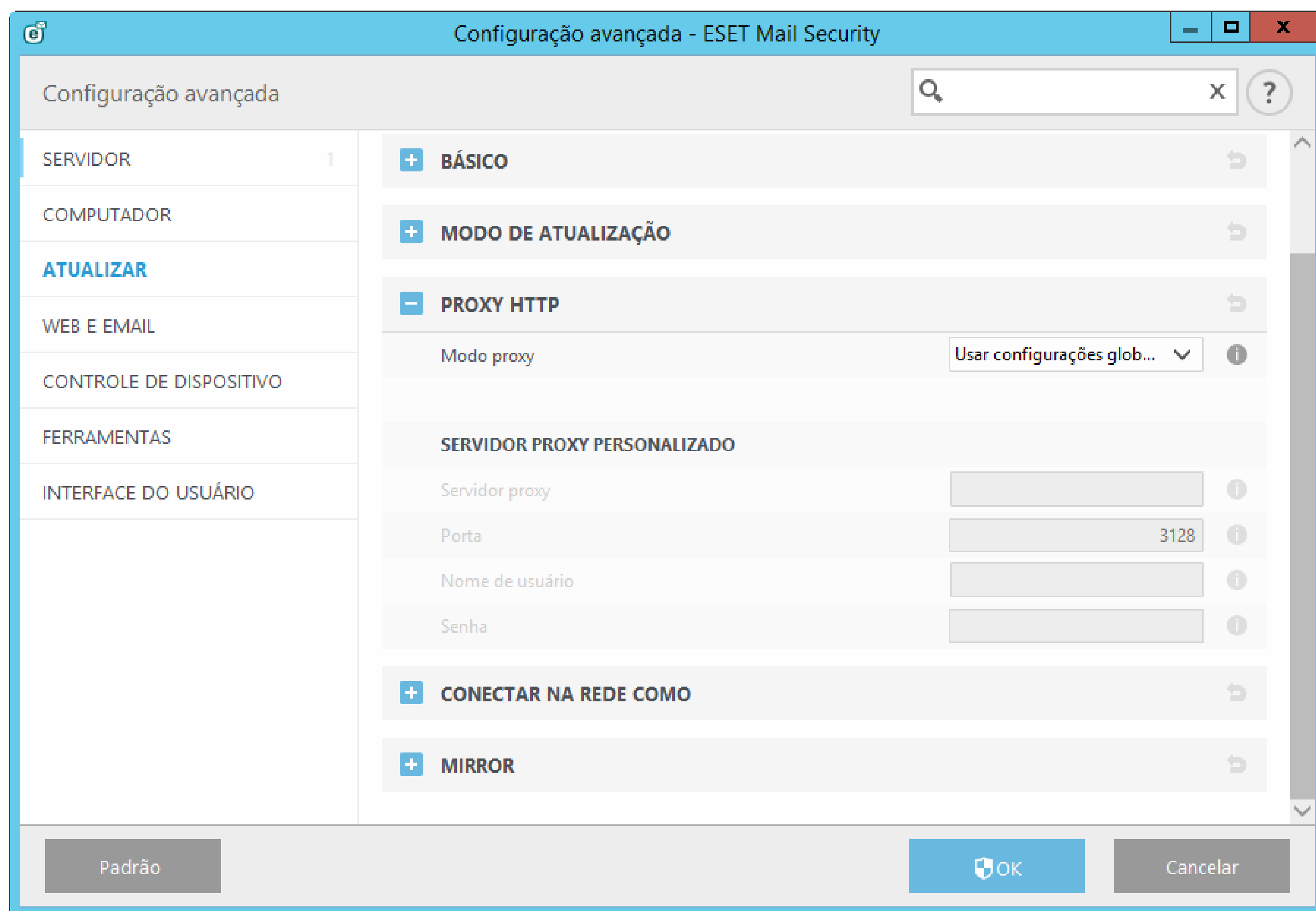
- Deve ser usado um servidor proxy para atualizar o ESET Mail Security que seja diferente do servidor proxy especificado nas configurações globais (**Ferramentas** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação (por padrão, 3128), além do **Usuário** e **Senha** para o servidor proxy, se necessário.
- As configurações do servidor proxy não foram definidas globalmente, mas o ESET Mail Security irá estabelecer conexão com um servidor proxy para atualizações.
- Seu computador estabelece conexão com a Internet por meio de um servidor proxy. As configurações são obtidas do Internet Explorer durante a instalação do programa; no entanto, se forem alteradas posteriormente (por exemplo, se você alterar o seu provedor de Internet), verifique se as configurações do proxy HTTP estão corretas nesta janela. Caso contrário, o programa não conseguirá estabelecer uma conexão com os servidores de atualização.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

i **OBSERVAÇÃO:** Os dados de autenticação, tais como **Usuário** e **Senha**, são destinados para acessar o servidor proxy. Preencha esses campos somente se um nome de usuário e uma senha forem necessários. Observe que esses campos não são para seu nome de usuário/senha do ESET Mail Security e devem ser fornecidos somente se você souber que precisa de senha para acessar a Internet por meio de um servidor proxy.

5.3.4 Conectar na rede como

Ao atualizar a partir de um servidor local com uma versão do sistema operacional Windows NT, a autenticação para cada conexão de rede é necessária por padrão.



Para configurar uma conta deste tipo, selecione a partir do menu suspenso **Tipo de usuário local**:

- **Conta do sistema (padrão)**,
- **Usuário atual**,
- **Usuário especificado**.

Selecione a opção **Conta do sistema (padrão)** para utilizar a conta do sistema para autenticação. De maneira geral, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa é autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação. Use esse método quando a conexão com a conta do sistema padrão falhar. Lembre-se de que a conta do usuário especificado deve ter acesso ao diretório de arquivos de atualização no servidor local. Caso contrário, o programa não poderá estabelecer conexão e fazer download das atualizações.

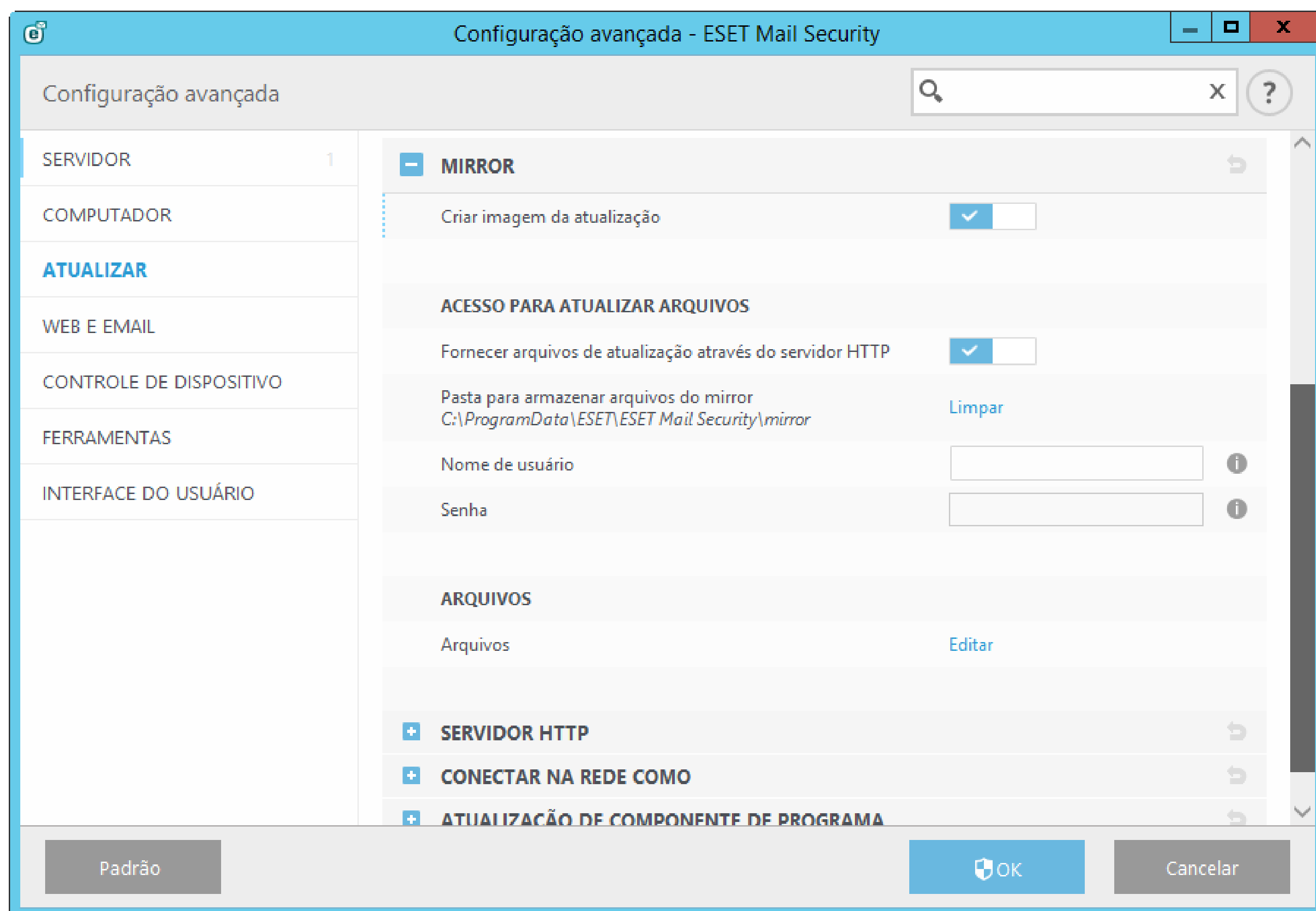
Aviso: Quando a opção **Usuário atual** ou **Usuário especificado** estiver selecionada, um erro poderá ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: *nome_domínio\usuário* (se for um grupo de trabalho, insira o *nome_do_grupo_de_trabalho\nome*) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

Selecione **Desconectar do servidor depois da atualização** para forçar uma desconexão se a conexão com o servidor permanecer ativa mesmo depois de fazer o download das atualizações.

5.3.5 Mirror

O ESET Mail Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outras estações de trabalho na rede. Uso de uma *"imagem"* - uma cópia dos arquivos de atualização no ambiente de rede local é conveniente, pois os arquivos de atualização não precisam ser obtidos por download a partir do servidor de atualização do fabricante repetidamente e por cada estação de trabalho. O download das atualizações é feito para o servidor de imagem local e, em seguida, distribuído a todas as estações de trabalho, evitando assim o risco de sobrecarga potencial do tráfego de rede. A atualização das estações clientes a partir de uma Imagem otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração do servidor local da Imagem estão localizadas em Configuração avançada em **Atualizar**. Para acessar esta seção pressione F5 para acessar a Configuração avançada, clique em **Atualizar** e selecione a guia **Imagem**.



Para criar uma imagem na estação de trabalho do cliente, ative **Criar imagem da atualização**. Ativar essa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Acesso para atualizar arquivos

Fornecer arquivos de atualização através do servidor HTTP interno - Se esta opção for ativada, os arquivos de atualização podem simplesmente ser acessados através de HTTP, sem a necessidade de credenciais.

OBSERVAÇÃO: O Windows XP precisa do Service Pack 2 ou posterior para usar o Servidor HTTP.

Os métodos de acesso do servidor de Imagem estão descritos em detalhes na seção Atualização através do Imagem. Há dois métodos básicos para acessar a Imagem - a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou os clientes podem acessar a imagem localizada em um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta** para procurar uma pasta no computador local ou em uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome de usuário** e **Senha**. Se a pasta de destino selecionada estiver localizada em um disco de rede que esteja executando o sistema operacional Windows NT/2000/XP, o nome de usuário e a senha especificados devem ter privilégios de gravação para a pasta selecionada. O nome de usuário e a senha devem ser inseridos no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Arquivos - Ao configurar a Imagem, é possível especificar as versões de idioma das atualizações que se deseja fazer download. Os idioma selecionados devem ser suportados pelo servidor de imagem configurado pelo usuário.

Servidor HTTP

Porta de servidor - Por padrão, a porta de servidor é definida como 2221.

Autenticação - Define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **Nenhum**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **NENHUM**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Acrescente o **Arquivo de encadeamento do certificado** ou gere um certificado assinado automaticamente caso deseje executar o servidor HTTP com suporte HTTPS (SSL). Os seguintes tipos de certificado estão disponíveis: ASN, PEM e PFX. É possível fazer download dos arquivos de atualização através do protocolo HTTPS, que fornece mais segurança. É quase impossível rastrear transferências de dados e credenciais de login usando esse protocolo. A opção **Tipo de chave privada** é definida como **Integrada** por padrão, (portanto a opção de **Chave privada de arquivo** está desativada por padrão). Isso significa que a chave privada é uma parte do arquivo de encadeamento do certificado selecionado.

Conectar na rede como

Tipo de usuário local - As configurações **Conta do sistema (padrão)**, **Usuário atual** e **Usuário especificado** serão exibidas nos menus suspensos correspondentes. As configurações **Nome** e **Senha** são opcionais. Consulte Conectar na rede como.

Selecione **Desconectar do servidor depois da atualização** para forçar uma desconexão se a conexão com o servidor permanecer ativa depois de fazer o download das atualizações.

Atualização de componente de programa

Atualizar componentes automaticamente - Permite a instalação de novos recursos e atualizações para recursos existentes. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador.

Atualizar componentes agora - Atualiza seus componentes do programa para a versão mais recente.

5.3.5.1 Atualização através do Mirror

Existem dois métodos básicos para configurar uma Imagem, que é essencialmente um repositório onde os clientes podem fazer download de arquivos de atualização. A pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou como um servidor HTTP.

Acesso à Imagem utilizando um servidor HTTP interno

Essa é a configuração padrão especificada na configuração do programa predefinida. Para permitir o acesso à Imagem utilizando o servidor HTTP, navegue até **Configuração avançada** > **Atualizar** > **Imagem** e selecione **Criar imagem da atualização**.

Na seção **Servidor HTTP** da guia **Imagem**, é possível especificar a **Porta do servidor**, em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**. A opção **Autenticação** define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **Nenhum**, **Básico** e **NTLM**.

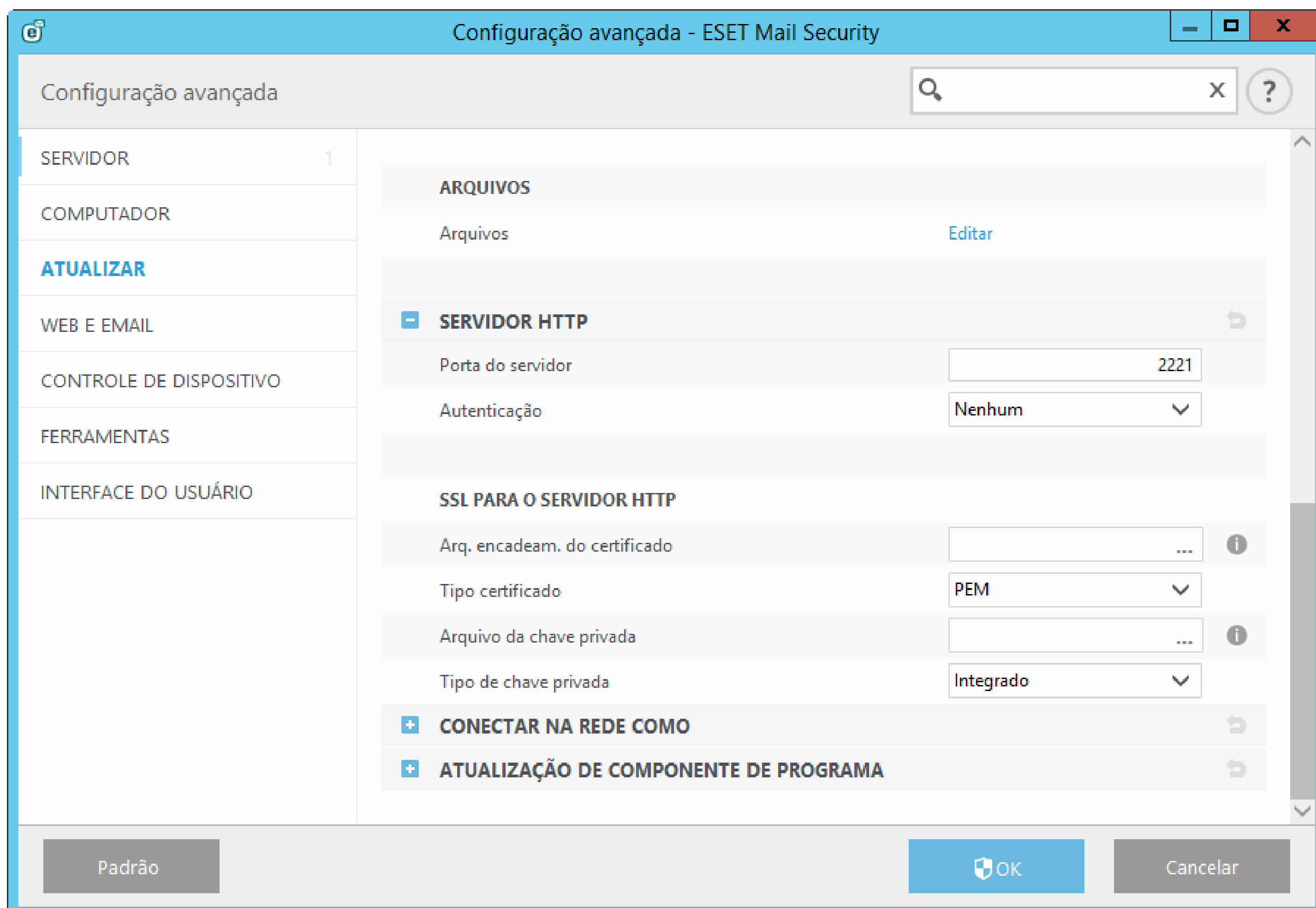
- Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha.
- A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado.
- A configuração padrão é **Nenhum**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Aviso: Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Imagem deve estar localizada no mesmo computador que a instância do ESET Mail Security que os criou.

SSL para o servidor HTTP

Acrescente o **Arquivo de encadeamento do certificado** ou gere um certificado assinado automaticamente caso deseje executar o servidor HTTP com suporte HTTPS (SSL). Os seguintes tipos de certificado estão disponíveis: **PEM, PFX** e **ASN**. É possível fazer download dos arquivos de atualização através do protocolo HTTPS, que fornece mais segurança. É quase impossível rastrear transferências de dados e credenciais de login usando esse protocolo. A opção **Tipo chave privada** é definida como **Integrada** por padrão, o que significa que a chave privada é uma parte do arquivo de encadeamento do certificado selecionado.

OBSERVAÇÃO: Um erro **Nome de usuário e/ou senha inválidos** aparecerá no Painel de atualização a partir do menu principal após diversas tentativas mal sucedidas de atualizar o banco de dados de assinatura de vírus a partir da Imagem. Recomendamos ir para **Configuração avançada** > **Atualizar**> **Imagem** e verificar o Nome de usuário e a Senha. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos.



Após concluir a configuração do servidor de Imagem, você deve adicionar o novo servidor de atualização em estações de trabalho clientes. Para fazer isso, siga as etapas a seguir:

- Acesse **Configuração avançada** (F5) e clique em **Atualizar** > **Básico**.
- Desative **Escolher automaticamente** e adicione um novo servidor ao campo **Servidor de atualização** usando um dos formatos a seguir:
  http://endereço_IP_do_seu_servidor:2221
  https://IP_address_of_your_server:2221 (se SSL for usado)

Acesso à Imagem por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um dispositivo de rede ou local. Ao criar a pasta para a Imagem, é necessário fornecer acesso de *"gravação"* para o usuário que salvará os arquivos de atualização na pasta e acesso de *"leitura"* para todos os usuários que atualizarão o ESET Mail Security a partir da pasta Imagem.

Depois configure o acesso à Imagem na guia **Configuração avançada** > **Atualizar**> **Imagem** desativando a opção **Fornecer arquivos atualizados através do servidor HTTP interno**. Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, será necessário inserir os dados de autenticação para acessar o outro computador. Para inserir os dados de autenticação, abra a Configuração avançada do ESET Mail Security (F5) e clique em **Atualizar** > **Conectar na rede como**. Essa configuração é a mesma para a atualização, conforme descrito na seção Conectar na rede como.

Após concluir a configuração da Imagem, prossiga até as estações de trabalho e configure *\\UNC\PATH* como o servidor de atualização usando estas etapas:

1. Abra o ESET Mail Security **Configuração avançada** e clique em **Atualizar** > **Básico**.
2. Clique em **Servidor de atualização** e adicione um novo servidor usando o formato *\\UNC\PATH*.

OBSERVAÇÃO: Para o funcionamento correto das atualizações, o caminho para a pasta Imagem deve ser especificado como um caminho UNC. A atualização das unidades mapeadas pode não funcionar.

A última seção controla os componentes do programa (PCUs). Por padrão, os componentes de programas baixados são preparados para copiar para a imagem local. Se **Atualizar componentes do programa** estiver ativado, não é necessário clicar em **Atualizar** porque os arquivos são copiados para a imagem local automaticamente quando estiverem disponíveis. Consulte Modo de atualização para obter mais informações sobre as atualizações dos componentes do programa.

5.3.5.2 Arquivos de imagem

Lista de arquivos componentes de programa disponíveis e localizados.

5.3.5.3 Solução de problemas de atualização através da Mirror

Na maioria dos casos, os problemas que ocorrem durante a atualização do servidor de Mirror são causados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Imagem, dados de autenticação incorretos para a pasta Imagem, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização a partir da Imagem ou por uma combinação das razões citadas. Aqui é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Mirror:

- O **ESET Mail Security relata um erro ao conectar a um servidor de imagem** - provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no menu **Iniciar** do Windows, clique em **Executar**, insira o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.

- O **ESET Mail Security requer um nome de usuário e senha** - Provavelmente provocado por dados de autenticação incorretos (nome de usuário e senha) na seção de atualização. O nome do usuário e a senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, *Domínio/Nome de usuário* ou *Grupo de trabalho/Nome de usuário*, além das senhas correspondentes. Se o servidor de Mirror puder ser acessado por “Todos”, esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. “Todos” não significa qualquer usuário não autorizado, apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta puder ser acessada por “Todos”, um nome de usuário e uma senha ainda precisarão ser inseridos na seção de configuração da atualização.

- O **ESET Mail Security relata um erro ao conectar a um servidor de imagem** - A comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

5.3.6 Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas são ativadas no ESET Mail Security:

- **Atualização automática de rotina**
- **Atualizar automaticamente após a conexão dial-up ter sido estabelecida**
- **Atualizar automaticamente após logon do usuário**

Cada tarefa de atualização pode ser alterada de acordo com suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda deste guia.

5.4 Web e email

A seção **Web e email** permite configurar a Proteção do cliente de email, proteger sua comunicação com a Internet usando a Proteção do acesso à web e controlar os protocolos da Internet configurando a Filtragem de protocolo. Esses recursos são cruciais para a proteção de seu computador durante a comunicação com a Internet.

A **Proteção do cliente de email** controla toda a comunicação por email, protege contra códigos maliciosos e permite escolher a ação que deverá ser aplicada quando uma infecção for detectada.

A **Proteção do acesso à Web** monitora a comunicação entre os navegadores da Internet e os servidores remotos e funciona de acordo com as regras HTTP e HTTPS. Esse recurso também permite bloquear, permitir ou excluir determinados Endereços URL.

A **Filtragem de protocolo** é uma proteção avançada para os protocolos de aplicativo e é fornecida pelo mecanismo de rastreamento do ThreatSense. Este controle funciona automaticamente, independente do navegador da Internet ou do cliente de email que estiver sendo usado. Também funciona para as comunicações criptografadas (SSL).

5.4.1 Filtragem de protocolos

Filtragem de protocolo

A proteção antivírus para os protocolos dos aplicativos é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. A filtragem de protocolo funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. Para editar configurações criptografadas (SSL), acesse **Web e email** > **Verificação de protocolo SSL**.

Ativar filtragem de conteúdo do protocolo de aplicativo - Essa opção pode ser usada para desativar a filtragem de protocolo. Observe que muitos componentes do ESET Mail Security (Proteção do acesso à Web, Proteção de protocolos de email e Antiphishing) dependem disso e não funcionarão sem ele.

Aplicativos excluídos - Permite que você exclua endereços remotos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Endereços IP excluídos - Permite que você exclua aplicativos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Clientes Web e email - Opção usada somente em sistemas operacionais Windows; permite que você selecione aplicativos dos quais todo o tráfego será filtrado por filtragem de protocolo, independentemente das portas usadas.

Registrar informações necessárias para a ESET para suporte no diagnóstico de problemas de filtragem de protocolo - Permite o registro em relatório avançado de dados de diagnóstico; use essa opção somente quando solicitado pelo suporte da ESET.

5.4.1.1 Aplicativos excluídos

Para excluir da filtragem de conteúdo a comunicação de aplicativos específicos que possuem direito de acesso à rede, selecione-os na lista. A comunicação HTTP/POP3 dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos usar esta opção apenas para aplicativos que não funcionam corretamente se as suas comunicações estiverem sendo rastreadas.

Aplicativos e serviços que já tiverem sido afetados pela filtragem de protocolos serão automaticamente exibidos depois que você clicar em **Adicionar**.

Editar - Edite as entradas selecionadas da lista.

Remover - Remove as entradas selecionadas da lista.

5.4.1.2 Endereços IP excluídos

Endereços IP nesta lista serão excluídos da filtragem de conteúdo de protocolo. A comunicação HTTP/POP3/IMAP de/para os endereços selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção apenas para endereços conhecidos como sendo confiáveis.

Adicionar - Clique em adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra é aplicada.

Editar - Edite as entradas selecionadas da lista.

Remover - Remove as entradas selecionadas da lista.

5.4.1.3 Clientes Web e email

i **OBSERVAÇÃO:** Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 2008, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, a seção **Clientes web e de email** não está disponível.

Devido à enorme quantidade de códigos maliciosos circulando na Internet, a navegação segura é um aspecto muito importante na proteção do computador. As vulnerabilidades do navegador da Web e os links fraudulentos ajudam o código malicioso a entrar no sistema despercebido e é por isso que o ESET Mail Security se focaliza na segurança do navegador da web. Cada aplicativo que acessar a rede pode ser marcado como um navegador da Internet. Aplicativos que já usam protocolos para comunicação ou aplicativos do caminho selecionado podem ser adicionados na lista clientes de email e Web.

5.4.2 Verificação do protocolo SSL

O ESET Mail Security é capaz de verificar se há ameaças em comunicações que usam o protocolo SSL. É possível usar vários modos de rastreamento para examinar comunicações protegidas por SSL com certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Ativa filtragem de protocolo SSL - Se a filtragem de protocolo estiver desativada, o programa não rastreará as comunicações em SSL.

O **Modo de filtragem de protocolo SSL** está disponível nas seguintes opções:

- **Modo automático** - Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado como confiável (ele está na lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.
- **Modo interativo** - Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.

Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2 - A comunicação que utiliza a versão anterior do protocolo SSL será bloqueada automaticamente.

Certificado raiz

Certificado raiz - Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). **Adicionar o certificado raiz aos navegadores conhecidos** deve estar ativado. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (por exemplo, Opera e Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (por exemplo, no Internet Explorer).

Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado** > **Detalhes** > **Copiar para arquivo...** e importe-o manualmente para o navegador.

Validade do certificado

Caso o certificado não esteja validado por uma autoridade certificadora: em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis. Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria dos negócios de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se **Perguntar sobre validade do certificado** estiver selecionado (selecionado por padrão), o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Você pode selecionar **Bloquear a comunicação que utiliza o certificado** para sempre encerrar conexões criptografadas para sites com certificados não verificados.

Se o certificado não for válido ou estiver corrompido, isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos que você deixe a opção **Bloquear a comunicação que utiliza o certificado** selecionada.

A **Lista de certificados conhecidos** permite que você personalize o comportamento do ESET Mail Security para certificados SSL específicos.

5.4.2.1 Comunicação SSL criptografada



Se seu sistema estiver configurado para usar o rastreamento de protocolo SSL, em duas situações será exibida uma janela de diálogo solicitando que você escolha uma ação:

Primeiro, se um site usar um certificado inválido ou que não possa ser verificado e o ESET Mail Security estiver configurado para perguntar ao usuário nesses casos (por padrão, sim para certificados que não podem ser verificados e não para inválidos), uma caixa de diálogo perguntará ao usuário se ele deseja **Permitir** ou **Bloquear** a conexão.

Depois, se o **modo de filtragem de protocolo SSL** estiver definido como **Modo interativo**, uma caixa de diálogo para cada site perguntará se você deseja **Rastrear** ou **Ignorar** o tráfego. Alguns aplicativos verificam se o tráfego SSL não foi modificado ou inspecionado por outra pessoa, sendo que em tais casos o ESET Mail Security deve **Ignorar** esse tráfego para manter o aplicativo funcionando.

Em ambos os casos, o usuário pode escolher lembrar a ação selecionada. Ações salvas serão armazenadas na **Lista de certificados conhecidos**.

5.4.2.2 Lista de certificados conhecidos

A Lista de certificados conhecidos pode ser usada para personalizar o comportamento do ESET Mail Security para certificados SSL específicos, bem como para lembrar ações escolhidas se o Modo interativo estiver selecionado em modo de filtragem de protocolo SSL. A lista pode ser visualizada e editada em **Configuração avançada** (F5) > **Web e email** > **Verificação do protocolo SSL** > **Lista de certificados conhecidos**.

A janela **Lista de certificados conhecidos** consiste em:

Colunas

- **Nome** - Nome do certificado.
- **Emissor de certificado** - Nome do autor do certificado.
- **Assunto do certificado** - O campo de assunto identifica a entidade associada à chave pública armazenada no campo de chave pública do assunto.
- **Acesso** - Selecione **Permitir** ou **Bloquear** como a **Ação de acesso** para permitir/bloquear a comunicação protegida por este certificado, independentemente de sua confiabilidade. Selecione **Automático** para permitir certificados confiáveis e perguntar para não confiáveis. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.
- **Rastrear** - Selecione **Rastrear** ou **Ignorar** como a **Ação de rastreamento** para rastrear ou ignorar a comunicação protegida por esse certificado. Selecione **Automático** para rastrear no modo automático e perguntar no modo interativo. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Elementos de controle

- **Editar** - Selecione o certificado que deseja configurar e clique em **Editar**.
- **Remover** - Selecione o certificado que deseja excluir e clique em **Remover**.
- **OK/Cancelar** - Clique em **OK** se quiser salvar alterações ou clicar em **Cancelar** se quiser sair sem salvar.

5.4.3 Proteção de cliente de email

A integração do ESET Mail Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Mail Security. Quando a integração for ativada, a barra de ferramentas do ESET Mail Security será inserida diretamente no cliente de email (a barra de ferramentas para versões mais recentes do Windows Live Mail não é inserida), permitindo proteção mais eficiente aos emails. As configurações de integração estão localizadas em **Configuração** > **Configuração avançada** > **Web e email** > **Proteção do cliente de email** > **Clientes de email**.

Integração com clientes de email

Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o rastreamento de vírus. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da Base de conhecimento da ESET.

Mesmo se a integração não estiver ativada, as comunicações por email ainda estarão protegidas pelo módulo de proteção do cliente de email (POP3, IMAP).

Ative a opção **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao

trabalhar com o seu cliente de email (somente para MS Outlook). Essa situação pode ocorrer ao recuperar emails do Kerio Outlook Connector Store.

Email para ser rastreado

Email recebido - Alterna a verificação das mensagens recebidas.
Email enviado - Alterna a verificação das mensagens enviadas.
Email lido - Alterna a verificação das mensagens lidas.

Ação que será executada no email infectado

Nenhuma ação - Se ativada, o programa identificará anexos infectados, mas não será tomada qualquer ação em relação aos emails.
Excluir email - O programa notificará o usuário sobre infiltrações e excluirá a mensagem.
Mover email para a pasta Itens excluídos - Os emails infectados serão movidos automaticamente para a pasta Itens excluídos.
Mover email para a pasta - Os emails infectados serão movidos automaticamente para a pasta especificada.

Pasta - Especifique a pasta personalizada para a qual você deseja mover os emails infectados quando detectados.

Repetir o rastreamento após atualização - Alterna o rastreamento depois de uma atualização do banco de dados de assinatura de vírus.

Aceitar resultados de rastreamento de outros módulos - Se essa opção for selecionada, o módulo de proteção do email aceitará os resultados de rastreamento de outros módulos de proteção (rastreamento de aplicativos POP3, IMAP).

5.4.3.1 Protocolos de email

Os protocolos IMAP e POP3 são os protocolos mais amplamente utilizados para receber comunicação em um aplicativo cliente de email. O ESET Mail Security fornece proteção para estes protocolos, independentemente do cliente de email usado, sem necessidade de reconfiguração do cliente de email.

Você pode configurar a verificação de protocolos IMAP/IMAPS e POP3/POP3S na Configuração avançada. Para acessar essa configuração, expanda **Web e email** > **Proteção do cliente de email** > **Protocolos de email**.

O ESET Mail Security também é compatível com o rastreamento de protocolos IMAPS e POP3S, que utilizam um canal criptografado para transferir as informações entre servidor e cliente. O ESET Mail Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa rastreará somente tráfego em portas definidas em portas usadas pelo protocolo IMAPS/POP3S, independentemente da versão do sistema operacional.

Comunicações criptografadas não serão rastreadas quando as configurações padrão estiverem em uso. Para ativar o rastreamento da comunicação criptografada, acesse Verificação de protocolo SSL em Configuração avançada, clique em **Web e email** > **Verificação de protocolo SSL** e selecione **Ativar filtragem de protocolo SSL**.

5.4.3.2 Alertas e notificações

A proteção de email fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP. Usando o plug-in para Microsoft Outlook e outros clientes de email, o ESET Mail Security permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP). Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado inclusos no mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com o banco de dados de assinaturas de vírus. O rastreamento das comunicações por protocolos POP3 e IMAP é independente do cliente de email usado.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** em **Web e email** > **Proteção do cliente de email** > **Alertas e notificações**.

Parâmetros ThreatSense - A configuração avançada do rastreamento de vírus permite configurar alvos do rastreamento, métodos de detecção, etc. Clique para exibir a janela de configuração do rastreamento de vírus

detalhada.

Depois que um email tiver sido verificado, uma notificação com o resultado da verificação pode ser anexada à mensagem. É possível selecionar **Acrescentar mensagem de marca nos emails recebidos e lidos, Acrescentar observação ao assunto de email infectado recebido e lido** ou **Acrescentar mensagens de marca a email enviado**. Esteja ciente que em algumas ocasiões mensagens de marca podem ser omitidas em mensagens HTML problemáticas ou se mensagem forem forjadas por malware. As mensagens de marca podem ser adicionadas a um email recebido e lido ou a um email enviado, ou ambos. As opções disponíveis são:

- **Nunca** - nenhuma mensagem de marca será adicionada.
- **Somente para email infectado** - Somente mensagens contendo software malicioso serão marcadas como rastreadas (padrão).
- **Para todos os emails rastreados** - o programa anexará mensagens a todos os emails rastreados.

Acrescentar observação ao assunto de email infectado enviado - Desative essa opção se você quiser que a proteção de email inclua um alerta de vírus no assunto de um email infectado. Esse recurso permite a filtragem simples com base em assunto de email infectado (se compatível com o seu programa de email). Esse recurso aumenta o nível de credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

Modelo adicionado ao assunto de email infectado - Edite esse modelo se desejar modificar o formato de prefixo do assunto de um email infectado. Essa função substituirá o assunto da mensagem *"Olá"* com o prefixo *"[vírus]"* para o seguinte formato: *"[virus] Olá"*. A variável *%VIRUSNAME%* representa a ameaça detectada.

5.4.3.3 Barra de ferramentas do MS Outlook

A proteção do Microsoft Outlook funciona como um módulo de plug-in. Após a instalação do ESET Mail Security, essa barra de ferramentas contendo as opções de proteção de antivírus é adicionada ao Microsoft Outlook:

ESET Mail Security - Clique no ícone para abrir a janela do programa principal do ESET Mail Security.

Rastrear novamente mensagens - Permite iniciar o rastreamento de emails manualmente. Você pode especificar as mensagens que serão verificadas e ativar o novo rastreamento do email recebido. Para obter mais informações, consulte Proteção do cliente de email.

Configuração do rastreamento - Exibe as opções de configuração da Proteção do cliente de email.

5.4.3.4 Barra de ferramentas do Outlook Express e do Windows Mail

A proteção do Outlook Express e do Windows Mail funciona como um módulo de plug-in. Depois de instalar o ESET Mail Security, essa barra de ferramentas contendo as opções de proteção antivírus será adicionada ao Outlook Express ou Windows Mail:

ESET Mail Security - Clique no ícone para abrir a janela do programa principal do ESET Mail Security.

Rastrear novamente mensagens - Permite iniciar o rastreamento de emails manualmente. Você pode especificar as mensagens que serão verificadas e ativar o novo rastreamento do email recebido. Para obter mais informações, consulte Proteção do cliente de email.

Configuração do rastreamento - Exibe as opções de configuração da Proteção do cliente de email.

Interface do usuário

Personalizar aparência - A aparência da barra de ferramentas pode ser modificada para o seu cliente de email. Desmarque a opção para personalizar a aparência, independentemente dos parâmetros do programa de email.

Mostrar texto - Exibe as descrições dos ícones.

Texto à direita - As descrições da opção são movidas da parte inferior para o lado direito dos ícones.

Ícones grandes - Exibe ícones grandes para as opções de menu.

5.4.3.5 Caixa de diálogo de confirmação

Esta notificação serve para confirmar que o usuário realmente deseja realizar a ação selecionada, que deve eliminar possíveis erros.

Por outro lado, a caixa de diálogo também oferece a opção de desativar as confirmações.

5.4.3.6 Rastrear novamente mensagens

A barra de ferramentas do ESET Mail Security integrada em clientes de email permite que os usuários especifiquem diversas opções para a verificação de email. A opção **Rastrear novamente mensagens** fornece dois modos de rastreamento:

Todas as mensagens na pasta atual - Rastreia as mensagens na pasta exibida no momento.

Apenas as mensagens selecionadas - Rastreia apenas as mensagens marcadas pelo usuário.

A caixa de seleção **Rastrear novamente as mensagens já rastreadas** possibilita ao usuário executar outro rastreamento nas mensagens que já foram rastreadas.

5.4.4 Proteção do acesso à web

A conectividade com a Internet é um recurso padrão na maioria de computadores pessoais. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. A proteção do acesso à Web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPS (comunicação criptografada).

O acesso à páginas da Web conhecidas como tendo conteúdo malicioso é bloqueado antes que o conteúdo seja baixado. Todas as outras páginas da Web serão rastreadas pelo mecanismo de rastreamento ThreatSense quando forem carregadas e bloqueadas se conteúdo malicioso for detectado. A proteção do acesso à Web oferece dois níveis de proteção, bloqueio por lista de proibições e bloqueio por conteúdo.

Recomendamos enfaticamente que você mantenha a proteção do acesso à Web ativada. Essa opção pode ser acessada a partir da janela do programa principal do ESET Mail Security localizada em **Configuração** > **Web e email** > **Proteção do acesso à Web**.

As seguintes opções estão disponíveis em **Configuração avançada** (F5) > **Web e email** > **Proteção do acesso à Web**:

- **Protocolos da Web** - Permite que você configure o monitoramento para esses protocolos padrão, que são usados pela maioria dos navegadores de Internet.
- **Gerenciamento de endereços URL** - Permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação.
- **Configuração de parâmetros do mecanismo ThreatSense** - Configuração avançada do rastreador de vírus - permite definir as configurações, como tipos de objetos para rastreamento (emails, arquivos, etc.), métodos de detecção para proteção do acesso à Web, etc.

5.4.4.1 Gerenciamento de endereços de URL

O gerenciamento de endereços URL permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação.

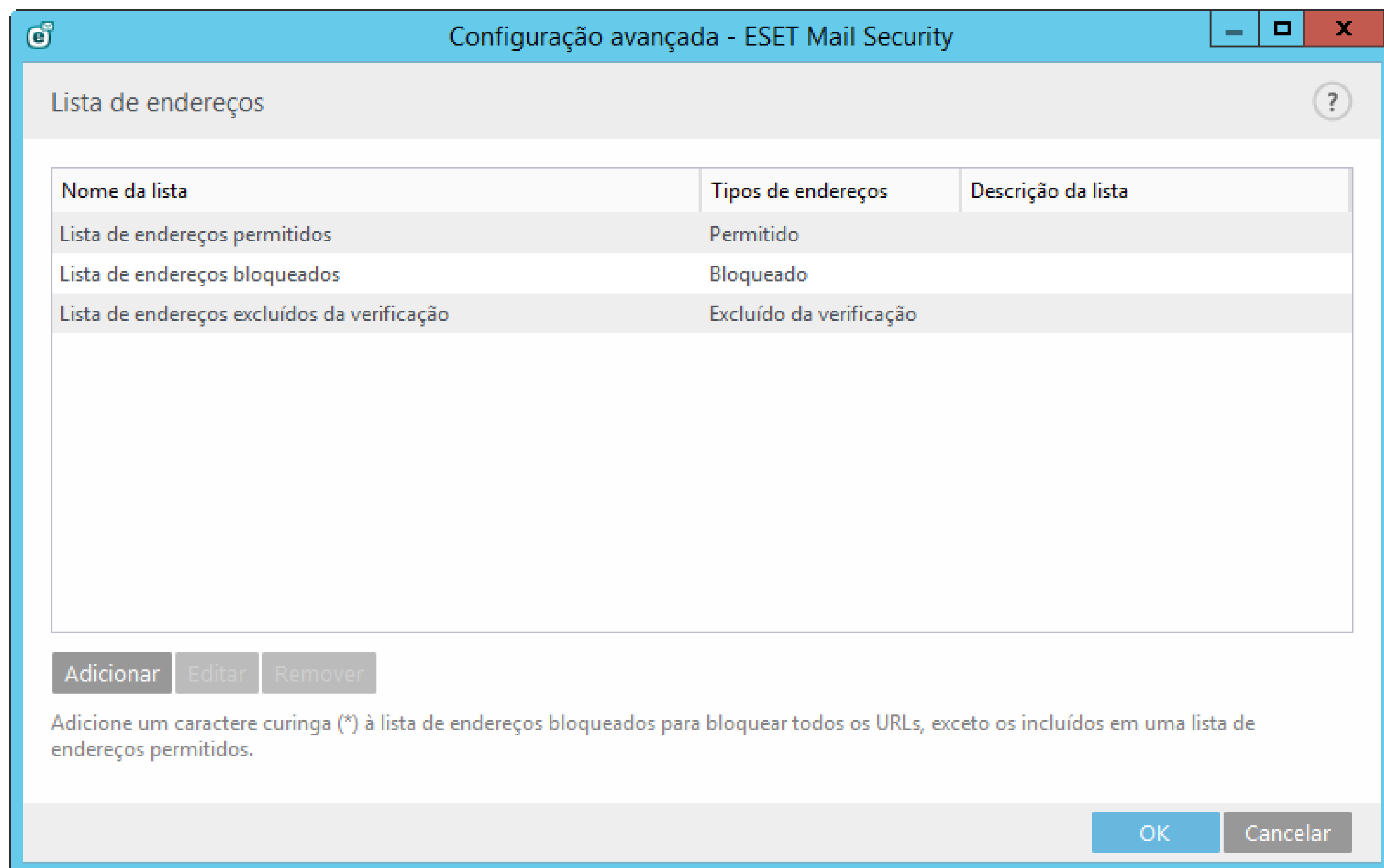
Sites na Lista de endereços bloqueados não estarão acessíveis, exceto se também forem incluídos na Lista de endereços permitidos. Sites na Lista de endereços excluídos da verificação não serão rastreados quanto a código malicioso quando acessados.

A opção **Ativar filtragem de protocolo SSL** deve ser selecionada se você quiser filtrar endereços HTTPS além de páginas HTTP. Caso contrário, somente os domínios de sites HTTPS que você tenha visitado serão adicionados, não a URL completa.

Em todas as listas, os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco representa qualquer número ou caractere, enquanto o ponto de interrogação representa qualquer caractere. Tenha

atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter apenas os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista.

Se você quiser bloquear todos os endereços HTTP, exceto endereços presentes na **Lista de endereços permitidos** ativa, adicione * à **Lista de endereços bloqueados** ativa.



Adicionar - Crie uma nova lista além das predefinidas. Isso pode ser útil se você quiser dividir logicamente diferentes grupos de endereços. Por exemplo, uma lista de endereços bloqueados pode conter endereços de alguma lista pública externa de proibições e uma segunda pode conter sua própria lista de proibições, que facilita a atualização da lista externa enquanto mantém a sua intacta.
Editar - Modifica listas existentes. Use isso para adicionar ou remover endereços das listas.
Remover - Exclui a lista existente. Possível somente para listas criadas com Adicionar, não para as padrão.

5.4.4.1.1 Criar nova lista

Essa seção permite especificar listas de endereços URL/máscaras que serão bloqueados, permitidos ou excluídos da verificação.

Ao criar uma nova lista, as seguintes opções estão disponíveis para configuração:

Tipo de lista de endereços - Três tipos de listas estão disponíveis:

- **Lista de endereços excluídos da verificação** - Nenhuma verificação quanto a código malicioso será realizada para qualquer endereço adicionado a essa lista.
- **Lista de endereços bloqueados** - O usuário não terá permissão para acessar endereços especificados nessa lista. Isso se aplica apenas ao protocolo HTTP. Protocolos que não o HTTP não serão bloqueados.
- **Lista de endereços permitidos** - Se Permitir acesso apenas a endereços HTTP na lista de endereços permitidos estiver ativada e a lista de endereços bloqueados tiver * (contém tudo), o usuário terá permissão para acessar apenas endereços especificados nessa lista. Os endereços nesta lista são permitidos mesmo se também estiverem presentes na lista de endereços bloqueados.

Nome da lista - Especifique o nome da lista. Esse campo estará esmaecido ao editar uma das três listas predefinidas.

Descrição da lista - Digite uma breve descrição para a lista (opcional). Esse campo estará esmaecido ao editar uma das três listas predefinidas.

Para ativar uma lista, selecione **Lista ativa** ao lado dessa lista. Se você quiser ser notificado quando uma lista específica for usada em avaliação de um site HTTP que você acessou, selecione **Notificar ao aplicar**. Por exemplo, uma notificação será emitida se um site for bloqueado ou permitido, pois está incluída na lista de endereços bloqueados ou permitidos. A notificação terá o nome da lista contendo o site especificado.

Adicionar - Adicione um novo endereço URL à lista (insira vários valores com separador).

Editar - Modifica endereço existente na lista. Somente possível para endereços criados com Adicionar.

Remover - Exclui endereços existentes na lista. Somente possível para endereços criados com Adicionar.

Importar - Importe um arquivo com endereços URL (separe os valores com uma quebra de linha, por exemplo, *.txt usando a codificação UTF-8).

5.4.4.1.2 Endereços HTTP

Nessa seção é possível especificar listas de endereços HTTP que serão bloqueados, permitidos ou excluídos da verificação.

Por padrão, as três listas a seguir estão disponíveis:

- **Lista de endereços excluídos da verificação** - Nenhuma verificação quanto a código malicioso será realizada para qualquer endereço adicionado a essa lista.
- **Lista de endereços permitidos** - Se **Permitir acesso apenas a endereços HTTP na lista de endereços permitidos** estiver ativada e a lista de endereços bloqueados tiver * (contém tudo), o usuário terá permissão para acessar apenas endereços especificados nessa lista. Os endereços nesta lista são permitidos mesmo se estiverem presentes na lista de endereços bloqueados.
- **Lista de endereços bloqueados** - O usuário não terá permissão para acessar endereços especificados nessa lista a menos que eles também estejam na lista de endereços permitidos.

Clique em **Adicionar** para criar uma nova lista. Para excluir as listas selecionadas, clique em **Remover**.

5.4.5 Proteção antiphishing

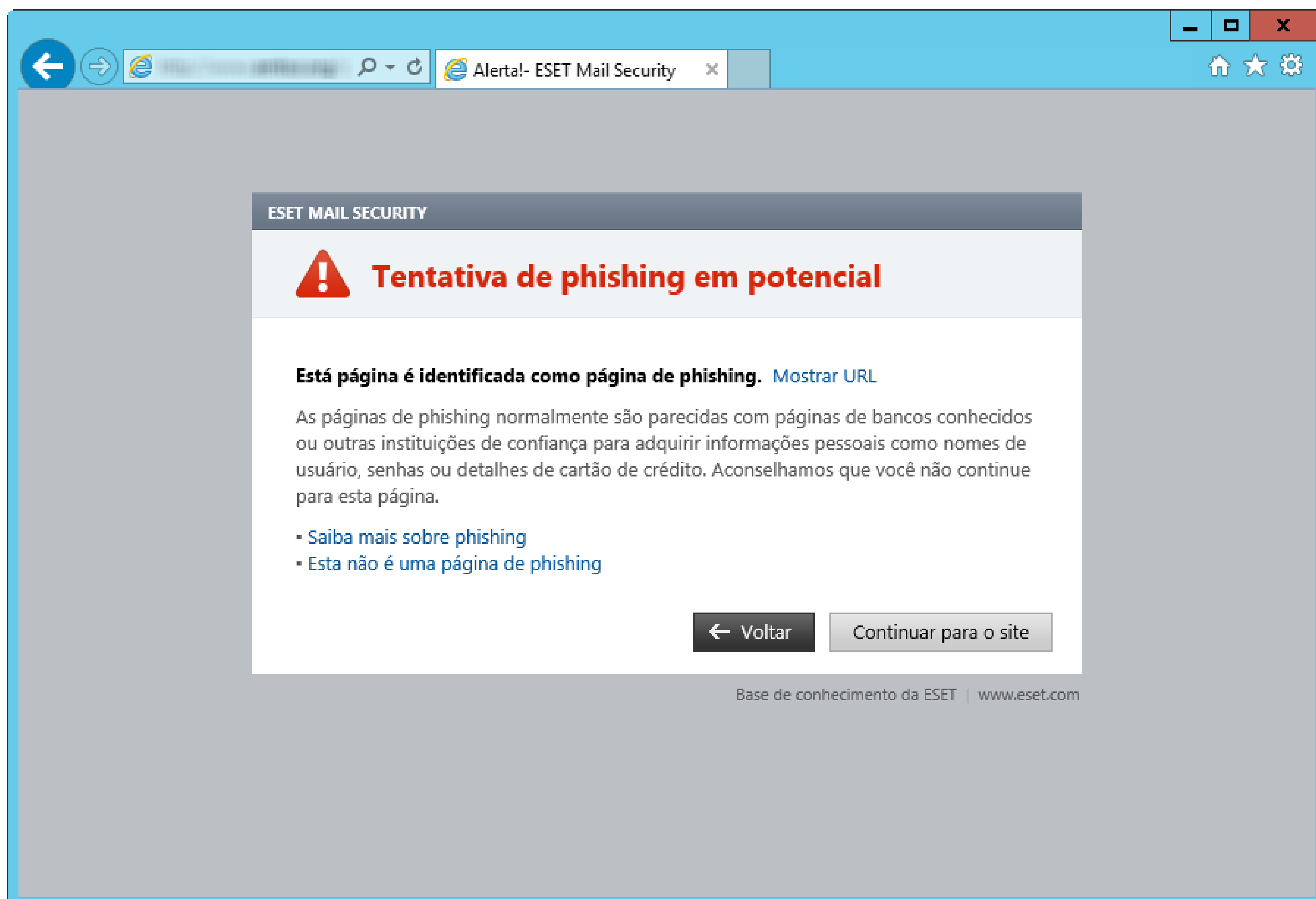
O termo roubo de identidade define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN e outros. Leia mais sobre essa atividade no glossário. O ESET Mail Security oferece proteção antiphishing; páginas da web conhecidas por distribuir esse tipo de conteúdo podem ser bloqueadas.

Recomendamos que você ative a proteção antiphishing no ESET Mail Security. Para isso, abra a **Configuração avançada** (F5) e vá para **Web e email** > **Proteção antiphishing**.

Visite nosso artigo da Base de conhecimento para mais informações sobre a Proteção antiphishing no ESET Mail Security.

Acessando um site de roubo de identidade

Ao acessar um site de roubo de identidade reconhecido, você verá a caixa de diálogo a seguir no seu navegador da web. Se ainda quiser ter acesso ao site, clique em **Continuar para o site** (não recomendável).



OBSERVAÇÃO: por padrão, sites de roubo de identidade em potencial que tiverem sido permitidos expirarão horas depois. Para permitir um site permanentemente, use a ferramenta de gerenciamento de endereços de URL. A partir de **Configuração avançada** (F5) abra **Web e email** > **Proteção do acesso à Web** > **Gerenciamento de endereços URL** > **Lista de endereços**, clique em **Editar** e adicione o site que deseja editar na lista.

Denúncia de site de roubo de identidade

O link Denunciar permite que você denuncie um site de phishing/malicioso para análise da ESET.

OBSERVAÇÃO: antes de enviar um site para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o site não foi detectado
- o site foi detectado incorretamente como uma ameaça. Nesse caso, é possível relatar um site de phishing falso positivo.

Como alternativa, você pode enviar o site por email. Envie seu email para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o site (por exemplo, o site do qual você foi enviado, como ouviu falar sobre ele, etc.).

5.5 Controle de dispositivos

O ESET Mail Security fornece controle automático de dispositivos (CD/DVD/USB/). Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo. Isso pode ser útil se a intenção do administrador do computador for evitar o uso de dispositivos com conteúdo não solicitado pelos usuários.

Dispositivos externos compatíveis:

- Armazenamento em disco (HDD, disco removível USB)
- CD/DVD
- Impressora USB
- Armazenamento de FireWire
- Dispositivo Bluetooth
- Leitor de cartão inteligente
- Dispositivo de imagens
- Modem
- Porta LPT/COM
- Dispositivos portáteis
- Todos os tipos de dispositivo

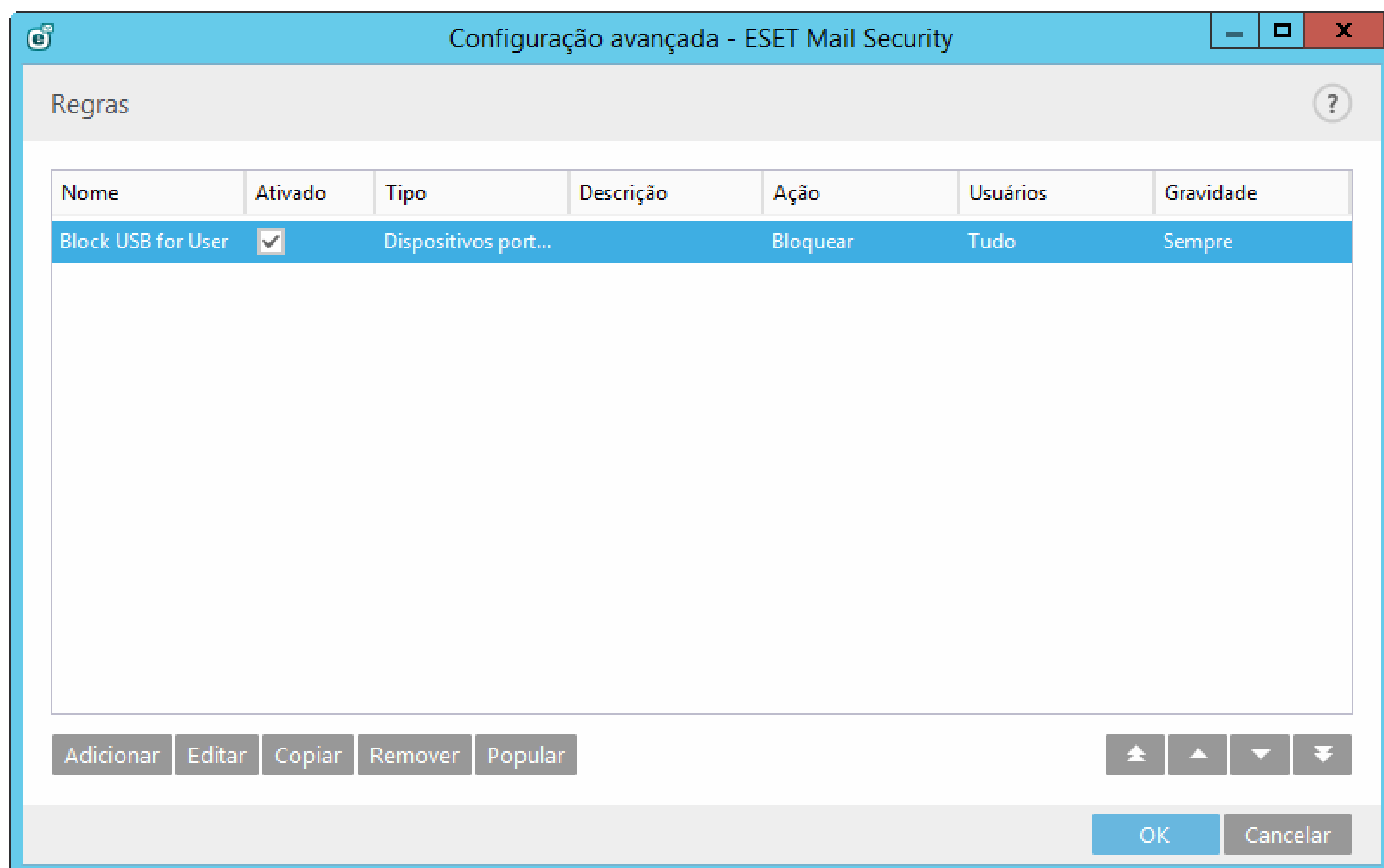
As opções de configuração do controle de dispositivos podem ser modificadas em **Configuração avançada** (F5) > **Controle de dispositivos**.

Ativar a opção ao lado de **Integrar no sistema** ativa o recurso de Controle de dispositivos no ESET Mail Security, você precisará reiniciar o computador para que as alterações tenham efeito. Quando o Controle de dispositivos estiver ativado, **Editor de regras** ficará ativo, permitindo abrir a janela do Editor de regras.

Se um dispositivo bloqueado por uma regra existente for inserido, uma janela de notificação será exibida e o acesso ao dispositivo não será concedido.

5.5.1 Regras do controle de dispositivos

A janela **Editor de regras do controle de dispositivos** mostra as regras existentes e permite que se controle de forma precisa os dispositivos externos que os usuários conectam ao computador.



Determinados dispositivos podem ser permitidos ou bloqueados por um usuário ou grupo de usuários e com base em parâmetros de dispositivos adicionais, que podem ser especificados na configuração da regra. A lista de regras contém diversas descrições de uma regra, tais como nome, o tipo de dispositivo externo, a ação a ser realizada após conectar um dispositivo externo ao seu computador e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique em **Remover** se quiser excluir a regra selecionada, ou desmarque a caixa de seleção **Ativado** ao lado de uma determinada regra para desativá-la. Isso pode ser útil se você não quiser excluir uma regra definitivamente, para poder usá-la no futuro.

Copiar - Cria uma nova regra com base nos parâmetros da regra selecionada.

Clique em **Preencher** para preencher automaticamente os parâmetros do dispositivo de mídia removível para dispositivos conectados ao computador.

As regras são listadas por ordem de prioridade, com regras de prioridade superior mais próximas do início. Você pode selecionar várias regras e aplicar ações, como excluí-las ou movê-las para cima ou para baixo na lista clicando em **Início/Para cima/Final/Para baixo** (botões de setas).

As entradas de relatórios podem ser visualizadas a partir da janela principal do programa do ESET Mail Security em **Ferramentas** > **Relatórios**.

5.5.2 Adição de regras do controle de dispositivos

Uma Regra de controle de dispositivos define a ação a ser tomada quando um dispositivo que corresponde aos critérios da regra é conectado ao computador.

Insira uma descrição da regra no campo **Nome** para melhor identificação. Clique na opção ao lado de **Regra ativada** para ativar ou desativar esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

Tipo de dispositivo

Escolha o tipo de dispositivo externo no menu suspenso (Armazenamento em disco/Dispositivo portátil/Bluetooth/FireWire/...). Os tipos de dispositivos são herdados do sistema operacional e podem ser visualizados no Gerenciador de dispositivos do sistema assumindo que um dispositivo esteja conectado ao computador. Os dispositivos de armazenamento incluem discos externos ou leitores de cartão de memória convencionais conectados via USB ou FireWire. Leitores de cartões inteligentes abrangem todos os leitores de cartões inteligentes com um circuito integrado incorporado, como cartões SIM ou cartões de autenticação. Scanners e câmeras são exemplos de dispositivos de imagens, eles não fornecem informações sobre os usuários, mas apenas sobre suas ações. Isto significa que os dispositivos de imagem só podem ser bloqueados a nível mundial.

Ação

O acesso a dispositivos que não sejam de armazenamento pode ser permitido ou bloqueado. Por outro lado, as regras de dispositivos de armazenamento permitem a seleção de uma das seguintes configurações de direitos:

- **Ler/Gravar** - Será permitido acesso total ao dispositivo.
- **Bloquear** - O acesso ao dispositivo será bloqueado.
- **Apenas leitura** - Será permitido acesso apenas para leitura ao dispositivo.

- **Alertar** - Cada vez que um dispositivo for conectado, o usuário será notificado se ele é permitido ou bloqueado, e um registro no relatório será feito. Dispositivos não são lembrados, uma notificação continuará a ser exibida com conexões subsequentes ao mesmo dispositivo.

Note que nem todos os direitos (ações) estão disponíveis para todos os tipos de dispositivos. Se um dispositivo tiver espaço de armazenamento, todas as quatro ações são disponibilizadas. Para dispositivos sem armazenamento, haverá somente duas (por exemplo, **Somente leitura** não estará disponível para Bluetooth, o que significa que dispositivos de Bluetooth poderão apenas ser permitidos ou bloqueados).

Outros parâmetros mostrados a seguir podem ser usados para ajustar as regras e adequá-las a dispositivos. Todos os parâmetros não fazem diferenciação entre letras maiúsculas e minúsculas:

- **Fabricante** - Filtragem por nome ou ID do fabricante.
- **Modelo** - O nome específico do dispositivo.
- **Número de série** - Os dispositivos externos geralmente têm seus próprios números de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD.

OBSERVAÇÃO: Se os três descritores estiverem vazios, a regra irá ignorar estes campos enquanto faz a correspondência. Os parâmetros de filtragem em todos os campos de texto não fazem diferenciação de maiúsculas e minúsculas; caracteres curinga (*, ?) não são aceitos.

Dica: Para descobrir os parâmetros de um dispositivo, crie uma regra para permitir o tipo de dispositivos, conecte o dispositivo ao seu computador e, em seguida, verifique os detalhes do dispositivo no Relatório de controle de dispositivos.

Gravidade

- **Sempre** - criar relatório de todos os eventos.
- **Diagnóstico** - Registra informações necessárias para ajustar o programa.
- **Informações** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Aviso** - Registra mensagens de erros críticos e de aviso.
- **Nenhum** - Nenhum registro será feito.

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à **Lista de usuários**:

- **Adicionar** - Abre os **Tipos de objeto: Usuários ou Grupos** que permite selecionar os usuários desejados.
- **Remover** - Remove o usuário selecionado do filtro.

i **OBSERVAÇÃO**: Todos os dispositivos podem ser filtrados por regras do usuário (por exemplo, dispositivos de criação de imagem não fornecem informações sobre usuários, apenas sobre ações invocadas).

5.5.3 Detectar dispositivos

O botão **Preencher** fornece uma visão geral de todos os dispositivos atualmente conectados com as informações a seguir: tipo de dispositivo, fabricante do dispositivo, modelo e número de série (se disponível). Ao selecionar um dispositivo (da lista de Dispositivos detectados) e clicar em **OK** , uma janela do editor de regras será exibida com informações predefinidas (todas as configurações podem ser ajustadas).

5.5.4 Grupos do dispositivo

 O dispositivo conectado ao seu computador pode representar um risco de segurança.

A janela Grupo de dispositivo é dividida em duas partes. A parte da direita da janela contém uma lista dispositivos que pertencem ao seu respectivo grupo e a parte da esquerda da janela contém uma lista de grupos existentes. Selecione um grupo que contenha os dispositivos que você deseja exibir no painel da direita.

Quando você abrir a janela Grupos do dispositivo e selecionar um grupo, poderá adicionar ou remover dispositivos da lista. Outra forma de adicionar dispositivos ao grupo é importá-los a partir de um arquivo. Alternativamente, você pode clicar em **Preencher** e todos os dispositivos conectados ao seu computador serão listados na janela **Dispositivos detectados**. Selecione um dispositivo da lista preenchida para adicioná-lo ao grupo ao clicar em **OK**.

Elementos de controle

Adicionar - Você pode adicionar um grupo ao inserir o nome, ou adicionar um dispositivo a um grupo existente. (opcionalmente, é possível especificar detalhes como nome do fornecedor, modelo e número de série) dependendo de onde na janela você clicou no botão.

Editar - Deixa você modificar o nome de um grupo ou parâmetros selecionados para os dispositivos aqui contidos (fabricante, modelo, número de série).

Remover - Exclui o grupo ou dispositivo selecionado dependendo de em qual parte da janela você clicou.

Importar - Importa uma lista de dispositivos de um arquivo.

O botão **Preencher** fornece uma visão geral de todos os dispositivos atualmente conectados com as informações a seguir: tipo de dispositivo, fabricante do dispositivo, modelo e número de série (se disponível).

Quando você tiver concluído a personalização, clique em **OK**. Clique em **Cancelar** se quiser deixar a janela **Grupo do dispositivo** sem salvar alterações.

DICA: É possível criar grupos diferentes de dispositivos para os quais regras diferentes serão aplicadas. Também é possível criar apenas um grupo de dispositivos para os quais a regra com ação **Ler/Gravar** ou **Apenas leitura** será aplicada. Isso garante que dispositivos não reconhecidos serão bloqueados pelo Controle de dispositivos quando conectados ao seu computador.

Note que nem todas as ações (permissões) estão disponíveis para todos os tipos de dispositivos. Para dispositivos de armazenamento, todas as quatro Ações estão disponíveis. Para dispositivos sem armazenamento, haverá somente duas (por exemplo, **Somente leitura** não estará disponível para Bluetooth, o que significa que dispositivos de Bluetooth poderão apenas ser permitidos, bloqueados ou alertados).

5.6 Ferramentas

O seguinte é a configuração avançada para todas as ferramentas que o ESET Mail Security oferece na guia **Ferramentas** na janela principal da interface gráfica do usuário.

5.6.1 ESET Live Grid

o ESET Live Grid é um sistema de avisos adiantado avançado composto de várias tecnologias baseadas na nuvem. Ele ajuda a detectar ameaças emergentes baseadas na reputação e melhora o desempenho de rastreamento através da lista de permissões. Informações sobre novas ameaças são enviadas em tempo real para a nuvem, o que permite que o ESET Malware Research Lab ofereça uma resposta oportuna e uniforme em todos os momentos. Os usuários podem verificar a reputação dos arquivos e dos processos em execução diretamente da interface do programa ou no menu de contexto, com informações adicionais disponíveis no ESET Live Grid. Ao instalar o ESET Mail Security, selecione uma das seguintes opções:

1. Você pode optar por não ativar o ESET Live Grid. Seu software não perderá nenhuma funcionalidade, mas, em alguns casos, o ESET Mail Security poderá responder mais devagar a novas ameaças do que a atualização do banco de dados de assinatura de vírus.
2. É possível configurar o ESET Live Grid para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça foi detectado. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ESET Live Grid coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Por padrão, o ESET Mail Security é configurado enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Os arquivos com certas extensões, como *.doc* ou *.xls*, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

O sistema de reputação do ESET Live Grid fornece lista de permissões e lista de proibições baseadas na nuvem. Para acessar configurações do ESET Live Grid, pressione F5 para acessar a Configuração avançada e expanda **Ferramentas** > **ESET Live Grid**.

Ativar o sistema de reputação ESET Live Grid (recomendado) - O sistema de reputação do ESET Live Grid melhora a eficiência de soluções anti-malware da ESET ao comparar os arquivos rastreados com um banco de dados de itens na lista de proibições e permissões da nuvem.

Enviar estatísticas anônimas - Permite que a ESET colete informações sobre ameaças recém-detectadas como o nome, data e hora de detecção da ameaça, método de detecção e metadados associados, versão e configuração do produto, inclusive informações sobre seu sistema.

Enviar arquivos - Arquivos suspeitos, que se pareçam com ameaças e/ou arquivos com características ou comportamento incomuns são enviados à ESET para análise.

Selecione **Ativar registro em relatório** para criar um relatório de eventos para registrar os envios de arquivos e informações estatísticas. Isso vai permitir o registro no Relatório de eventos quando as estatísticas ou os arquivos são enviados.

Email de contato (opcional) - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

Exclusão - O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Se já tiver usado o ESET Live Grid antes e o tiver desativado, ainda pode haver pacotes de dados a enviar. Mesmo depois da desativação, tais pacotes serão enviados à ESET. Assim que todas as informações atuais forem enviadas, não serão criados pacotes adicionais.

5.6.1.1 Filtro de exclusões

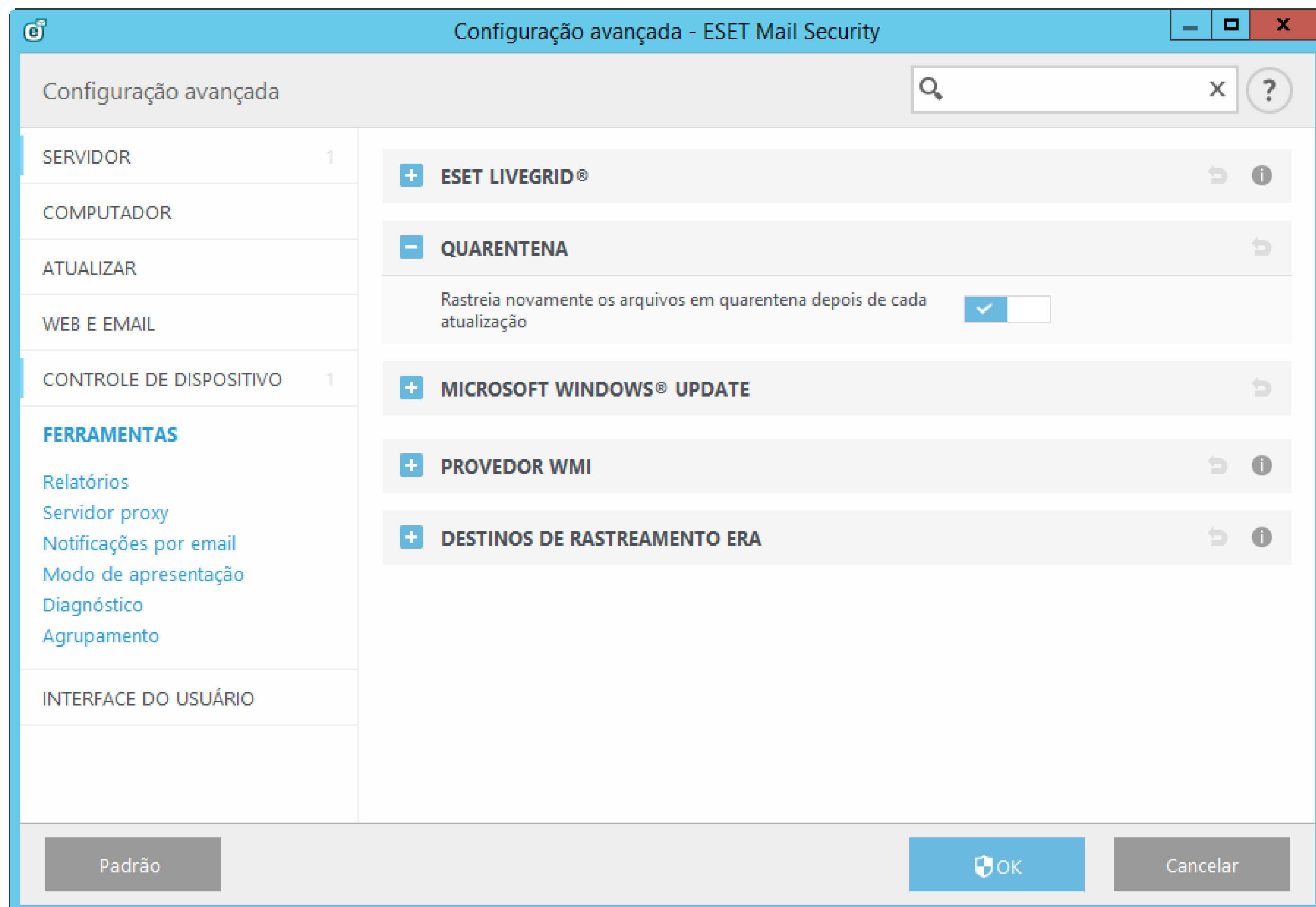
A opção **Editar**, ao lado de Exclusões no ESET Live Grid, permite configurar como as ameaças serão enviadas ao Laboratório de vírus da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de ameaças. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

5.6.2 Quarentena

Arquivos infectados ou suspeitos são armazenados de forma segura na pasta de quarentena. Por padrão, o módulo de proteção em tempo real coloca em quarentena todos os arquivos suspeitos criados recentemente para evitar infecção.

Rastrear novamente arquivos colocados em quarentena após cada atualização - Todos os objetos colocados em quarentena serão rastreados depois de cada atualização do banco de dados de assinatura de vírus. Isso é especialmente útil se um arquivo tiver sido movido para a quarentena em consequência de uma detecção que seja falso-positiva. Com essa opção ativada, determinados tipos de arquivos podem ser automaticamente restaurados para seu local original.



5.6.3 Microsoft Windows Update

Atualizações do Windows fornecem soluções importantes para vulnerabilidades potencialmente perigosas e melhora o nível de segurança geral do seu computador. Por esse motivo, é extremamente importante manter as atualizações do Microsoft Windows em dia, instalando-as assim que forem disponibilizadas. O ESET Mail Security o notificará sobre as atualizações ausentes de acordo com o nível que você especificar. Os seguintes níveis estão disponíveis:

- **Nenhuma atualização** - Nenhuma atualização de sistema será proposta para download.
- **Atualizações opcionais** - Atualizações marcadas como de baixa prioridade e superiores serão propostas para download.
- **Atualizações recomendadas** - Atualizações marcadas como comuns e superiores serão propostas para download.
- **Atualizações importantes** - Atualizações marcadas como importantes e superiores serão propostas para download.
- **Atualizações críticas** - Apenas atualizações críticas serão propostas para download.

Clique em **OK** para salvar as alterações. A janela Atualizações do sistema será exibida depois da verificação do status com o servidor de atualização. As informações sobre atualização de sistema podem não estar disponíveis imediatamente após as alterações serem salvas.

5.6.4 Provedor WMI

Sobre o WMI

A Instrumentação de gerenciamento do Windows (WMI) é a implementação do Gerenciamento corporativo com base na web (WBEM), que é uma iniciativa da indústria para desenvolver tecnologia padrão para acessar informações de gerenciamento em um ambiente corporativo.

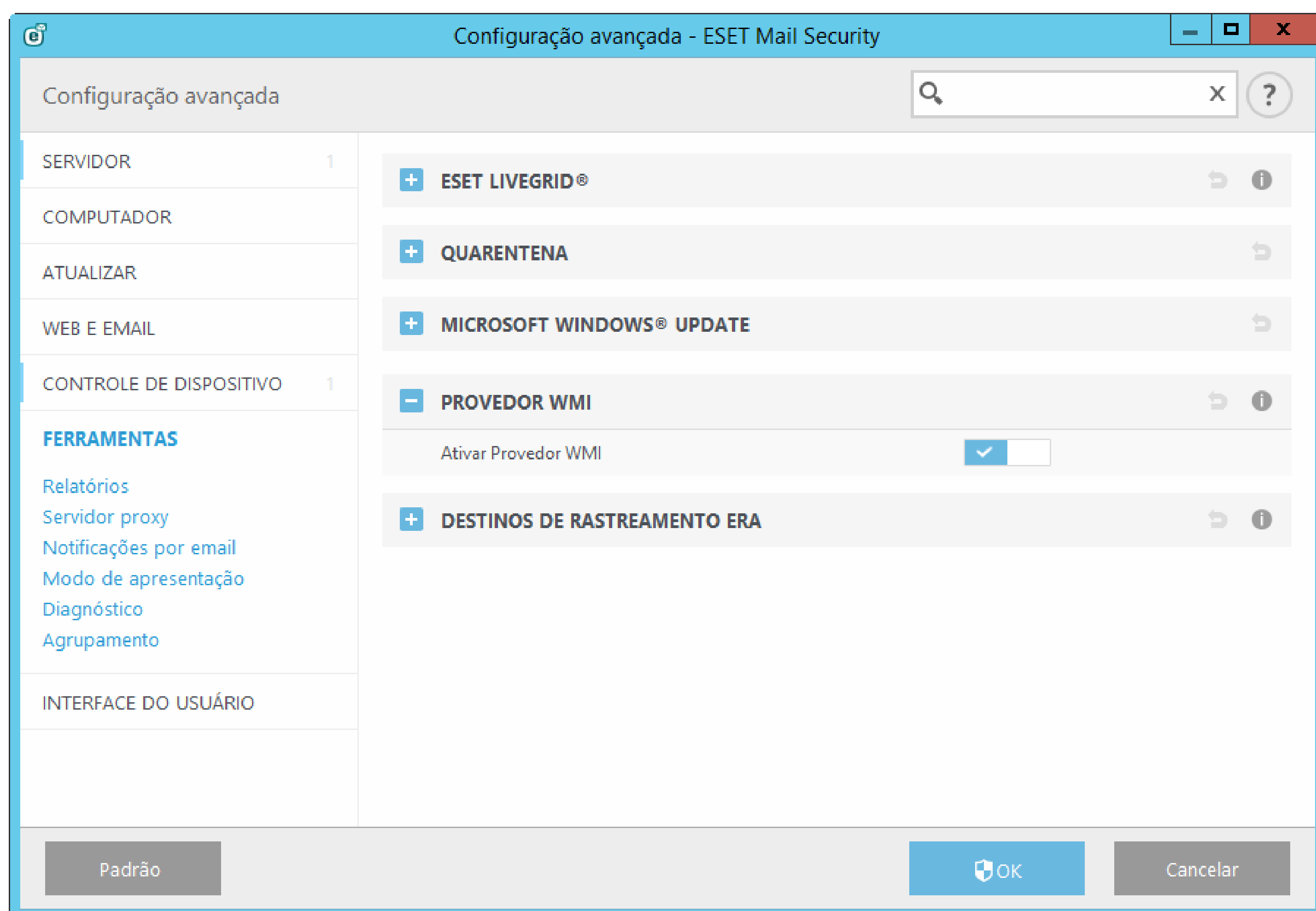
Para mais informações sobre o WMI, consulte http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

Provedor WMI ESET

O objetivo do Provedor WMI ESET é permitir o monitoramento remoto de produtos ESET em um ambiente representativo, sem a necessidade de software ou ferramentas específicas da ESET. Ao expor as informações básicas de produto, status e estatísticas através do WMI, nós aumentamos muito as possibilidades dos administradores de empresas ao monitorar os produtos ESET. Administradores podem aproveitar o número de métodos de acesso oferecidos pelo WMI (linha de comando, scripts e ferramentas de monitoramento de empresa de terceiros) para monitorar o estado de seus produtos ESET.

A implementação atual fornece acesso somente leitura a informações básicas do produto, recursos instalados e seu status da proteção, estatísticas de rastreamentos individuais e relatórios de produto.

O provedor WMI permite o uso da infraestrutura e ferramentas padrão Windows WMI para ler o estado do produto e os relatórios do produto.



5.6.4.1 Fornecer dados

Todas as classes WMI relacionadas a um produto ESET estão localizadas no namespace "root\ESET". As classes a seguir, que são descritas em mais detalhes abaixo, estão implementadas no momento:

Geral:

- ESET_Product
- ESET_Features
- ESET_Statistics

Relatórios:

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_GreylistLog
- ESET_SpamLog

Classe ESET_Product

Só pode haver uma instância da classe ESET_Product. Propriedades desta classe são referentes a informações básicas sobre seu produto ESET instalado:

- **ID** - Identificador do tipo de produto, por exemplo, "essbe"
- **Name** - nome do produto, por exemplo "ESET Security"
- **Edition** - edição do produto, por exemplo, "Microsoft SharePoint Server"
- **Version** - Versão do produto, por exemplo "4.5.15013.0"
- **VirusDBVersion** - versão do banco de dados de vírus, por exemplo "7868 (20130107)"
- **VirusDBLastUpdate** - registro da última atualização do banco de dados de vírus. A string contém o registro no formato de hora e data WMI, por exemplo, "20130118115511.000000+060"
- **LicenseExpiration** - tempo de expiração da licença. A string contém o registro no formato de hora e data WMI, por exemplo, "20130118115511.000000+060"
- **KernelRunning** - valor booleano indicando se o serviço eKrn está sendo executado na máquina, por exemplo, "VERDADEIRO"
- **StatusCode** - número indicando o status da proteção do produto: 0 - Verde (OK), 1 - Amarelo (Alerta), 2 - Vermelho (Erro)
- **StatusText** - mensagem descrevendo o motivo de um código de status não-zero, caso contrário ficará vazio

Classe ESET_Features

A classe ESET_Features tem várias instâncias, dependendo do número de recursos do produto. Cada instância contém:

- **Name**- Nome do recurso (lista de nomes fornecida abaixo)
- **Status** - Status do recurso: 0 - inativo, 1 - desativado, 2 - ativado

Uma lista de string representando os recursos de produtos reconhecidos no momento:

- **CLIENT_FILE_AV** - Proteção antivírus em tempo real do sistema de arquivos
- **CLIENT_WEB_AV** - proteção antivírus web do cliente
- **CLIENT_DOC_AV** - proteção antivírus de documento do cliente
- **CLIENT_NET_FW** - Firewall pessoal do cliente
- **CLIENT_EMAIL_AV** - proteção antivírus de email do cliente
- **CLIENT_EMAIL_AS** - proteção anti-spam de email do cliente
- **SERVER_FILE_AV** - proteção antivírus em tempo real de arquivos no produto de arquivo servidor protegido, por exemplo, arquivos no banco de dados de conteúdo do SharePoint no caso do ESET Mail Security
- **SERVER_EMAIL_AV** - proteção antivírus de emails do produto de servidor protegido, por exemplo, emails no MS Exchange ou IBM Lotus Domino
- **SERVER_EMAIL_AS** - proteção anti-spam de emails do produto de servidor protegido, por exemplo, emails no MS Exchange ou IBM Lotus Domino
- **SERVER_GATEWAY_AV** - proteção antivírus de protocolos de rede protegidos no gateway
- **SERVER_GATEWAY_AS** - proteção anti-spam de protocolos de rede protegidos no gateway

Classe ESET_Statistics

A classe ESET_Statistics tem várias instâncias, dependendo do número de rastreamentos no produto. Cada instância contém:

- Scanner - código string para o rastreamento em particular, por exemplo, "CLIENT_FILE"
- Total - número total de arquivos rastreados
- Infected - número de arquivos infectados encontrados
- Cleaned - número de arquivos limpos
- Timestamp - registro da última alteração nas estatísticas. No formato de hora e data WMI, por exemplo, "20130118115511.000000+060"
- ResetTime - registro de quando o contados de estatísticas foi redefinido mais recentemente. No formato de hora e data WMI, por exemplo, "20130118115511.000000+060"

Lista de strings representando os rastreamentos reconhecidos no momento:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

Classe ESET_ThreatLog

A classe ESET_ThreatLog tem várias instâncias, cada uma representando um registro de relatório do relatório “Ameaças detectadas”. Cada instância contém:

- **ID** - ID único deste registro de relatório
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **LogLevel** - gravidade do registro de relatório expressa como um número de [0-8]. Os valores correspondem aos níveis nomeados a seguir: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner** - Nome do rastreamento que criou este evento de relatório
- **ObjectType** - Tipo de objeto que produziu este evento de relatório
- **ObjectName** - Nome do objeto que produziu este evento de relatório
- **Threat** - Nome da ameaça encontrada no objeto descrito pelas propriedades ObjectName e ObjectType
- **Action** - Ação realizada depois da identificação da ameaça
- **User** - Conta do usuário que causou este evento de relatório
- **Information** - Descrição adicional do evento

ESET_EventLog

A classe ESET_EventLog tem várias instâncias, cada uma representando um registro de relatório do relatório de "Eventos". Cada instância contém:

- **ID** - ID único deste registro de relatório
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **LogLevel** - gravidade do registro de relatório expressa como um número no intervalo [0-8]. Os valores correspondem aos níveis nomeados a seguir: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Module** - Nome do módulo que criou este evento de relatório
- **Event** - Descrição do evento
- **User** - Conta do usuário que causou este evento de relatório

ESET_ODFileScanLogs

A classe ESET_ODFileScanLogs tem várias instâncias, cada uma representando um registro de arquivo de rastreamento sob demanda. Isto é equivalente à lista de relatórios "Rastreamento sob demanda do computador" na interface gráfica do usuário. Cada instância contém:

- **ID** - ID único deste relatório sob demanda
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **Targets** - Pastas/objetos de destino do rastreamento
- **TotalScanned** - Número total de objetos rastreados
- **Infected** - Número de objetos infectados encontrados
- **Cleaned** - Número de objetos limpos
- **Status** - Status do processo de rastreamento

ESET_ODFileScanLogRecords

A classe ESET_ODFileScanLogRecords tem várias instâncias, cada uma representando um registro de relatório em um dos relatórios de rastreamento representados por instâncias da classe ESET_ODFileScanLogs. Instâncias desta classe fornecem registros de relatório de todos os rastreamentos/relatórios sob demanda. Quando é necessária apenas uma instância de um relatório de rastreamento em particular, eles devem ser filtrados pela propriedade LogID. Cada instância de classe contém:

- **LogID** - ID do relatório de rastreamento ao qual este registro pertence (ID de uma das instâncias da classe ESET_ODFileScanLogs)
- **ID** - ID único deste registro de relatório de rastreamento
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **LogLevel** - gravidade do registro de relatório expressa como um número [0-8]. Os valores correspondem aos níveis nomeados a seguir: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - a mensagem de relatório real

ESET_ODServerScanLogs

A classe ESET_ODServerScanLogs tem várias instâncias, cada uma representando uma execução do rastreamento de servidor sob demanda. Cada instância contém:

- **ID** - ID único deste relatório sob demanda
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **Targets** - Pastas/objetos de destino do rastreamento
- **TotalScanned** - Número total de objetos rastreados
- **Infected** - Número de objetos infectados encontrados
- **Cleaned** - Número de objetos limpos
- **RuleHits** - Número de acessos de regra
- **Status** - Status do processo de rastreamento

ESET_ODServerScanLogRecords

A classe ESET_ODServerScanLogRecords tem várias instâncias, cada uma representando um registro de relatório em um dos relatórios de rastreamento representados por instâncias da classe ESET_ODServerScanLogs. Instâncias desta classe fornecem registros de relatório de todos os rastreamentos/relatórios sob demanda. Quando é necessária apenas uma instância de um relatório de rastreamento em particular, eles devem ser filtrados pela propriedade LogID. Cada instância de classe contém:

- **LogID** - ID do relatório de rastreamento ao qual este registro pertence (ID de uma das instâncias da classe ESET_ ODServerScanLogs)
- **ID** - ID único deste registro de relatório de rastreamento
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **LogLevel** - gravidade do registro de relatório expressa como um número no intervalo [0-8]. Os valores correspondem aos níveis nomeados a seguir: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log** - a mensagem de relatório real

ESET_GreylistLog

A classe ESET_GreylistLog tem várias instâncias, cada uma representando um registro de relatório do relatório de “Lista cinza”. Cada instância contém:

- **ID** - ID único deste registro de relatório
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **LogLevel** - gravidade do registro de relatório expressa como um número [0-8]. Os valores correspondem aos níveis nomeados a seguir: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain** - Nome do domínio HELO
- **IP** - Endereço IP de origem
- **Sender** - Remetente do email
- **Recipient** - Destinatário de email
- **Action** - Ação realizada
- **TimeToAccept** - Número de minutos depois do qual o email será aceito

ESET_SpamLog

A classe ESET_SpamLog tem várias instâncias, cada uma representando um registro de relatório de “Spamlog”. Cada instância contém:

- **ID** - ID único deste registro de relatório
- **Timestamp** - criação de um registro do relatório (no formato data/hora WMI)
- **LogLevel** - gravidade do registro de relatório expressa como um número [0-8]. Os valores correspondem aos níveis nomeados a seguir: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Sender** - Remetente do email
- **Recipients** - Destinatário de email
- **Subject** - Assunto do email
- **Received** - Hora do recebimento
- **Score** - Pontuação de spam em porcentagem [0-100]
- **Reason** - O motivo do email ter sido marcado como spam
- **Action** - Ação realizada
- **DiagInfo** - Informações adicionais de diagnóstico

5.6.4.2 Acessando dados fornecidos

Aqui estão alguns exemplos de como acessar os dados WMI da ESET a partir da linha de comando do Windows e de PowerShell, que deve ser possível a partir de qualquer sistema operacional atual do Windows. Porém, há muitas outras formas de acessar os dados a partir de outras linguagens de script e ferramentas.

Linha de comando sem scripts

O comando `wmic` a ferramenta linha de comando pode ser usada para acessar várias classes pré-definidas ou qualquer classe WMI personalizada.

Para exibir informações completas sobre o produto na máquina local:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Para exibir apenas o número de versão de produto do produto na máquina local:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Para exibir informações completas sobre o produto em uma máquina remota com IP 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Obter e exibir informações completas sobre o produto na máquina local:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Obter e exibir informações completas sobre o produto em uma máquina remota com IP 10.1.118.180:

```
$cred = Get-Credential            # pede as credenciais ao usuário e armazena-as na variável
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred $cred
```

5.6.5 Destinos de rastreamento ERA

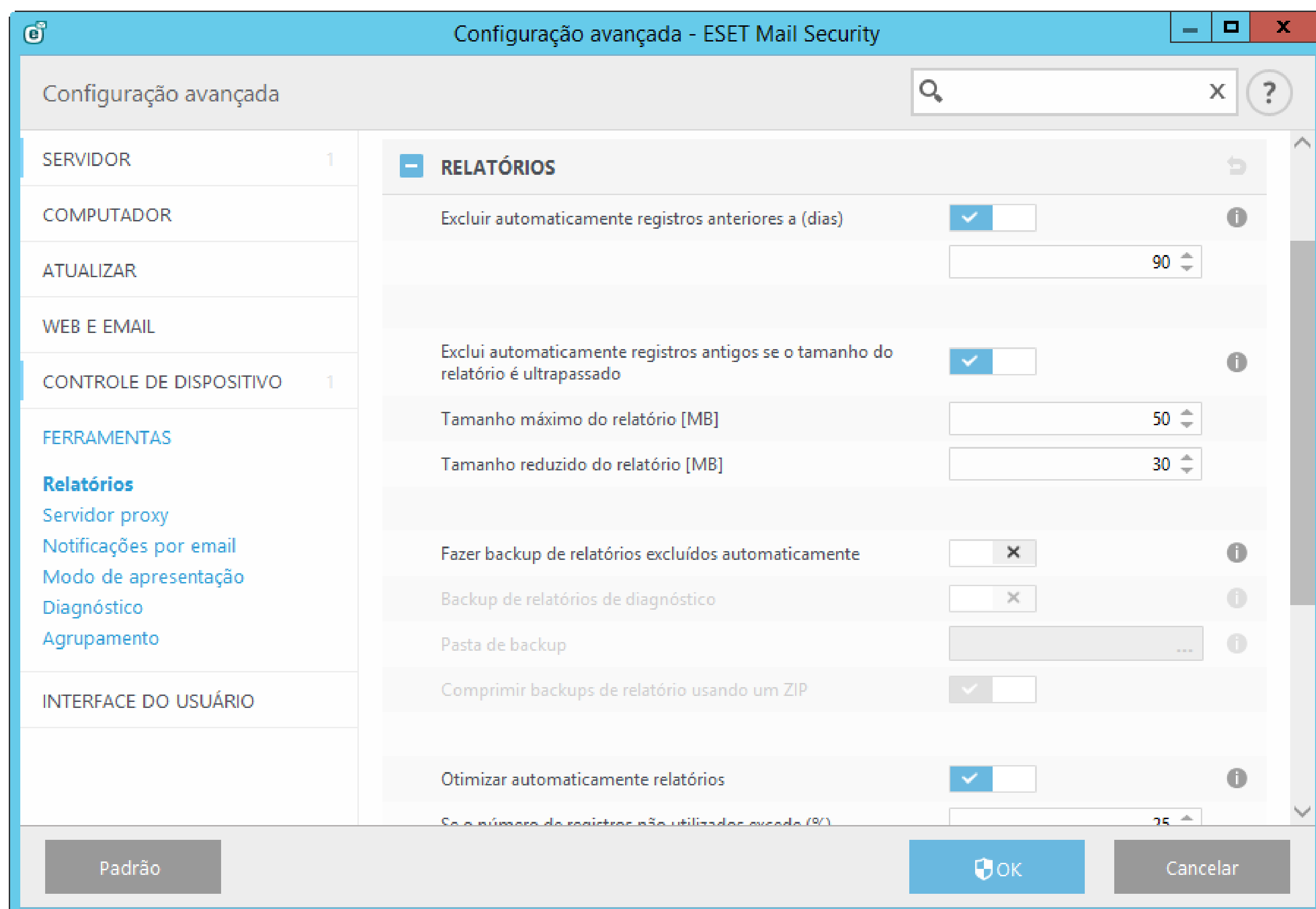
Essa funcionalidade permite que o ESET Remote Administrator use Destinos do banco de dados para rastreamento sob demanda adequados ao executar a tarefa de cliente **Rastrear servidor** em um servidor com ESET Mail Security.

Ao ativar a funcionalidade **Gerar lista de destino**, o ESET Mail Security cria uma lista de banco de dados de destinos de rastreamento disponíveis no momento. Essa lista é gerada periodicamente, de acordo com um **Período de atualização** definido em minutos. Quando o ERA deseja executar uma tarefa de cliente **Rastrear servidor**, ele vai coletar a lista e deixar você escolher os destinos de rastreamento para o Rastreamento sob demanda de banco de dados daquele servidor em particular.

5.6.6 Relatórios

A configuração de relatórios do ESET Mail Security pode ser acessada na janela principal do programa.

Clique em **Configuração** > **Configuração avançada** > **Ferramentas** > **Relatórios**. A seção de relatórios é utilizada para definir como os relatórios serão gerenciados. O programa exclui automaticamente os relatórios mais antigos a fim de economizar espaço no disco rígido.



5.6.6.1 Filtragem de relatórios

Registra em relatório as informações de armazenamento sobre eventos importantes do sistema. O recurso de filtragem de relatórios permite exibir registros sobre um tipo específico de evento.

Insira a palavra-chave no campo **Localizar texto**. Use o menu suspenso **Pesquisar nas colunas** para refinar sua pesquisa.

Tipos de registro - Escolha um ou mais tipos de relatório de registro no menu suspenso:

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus).

Período de tempo - Defina o período de tempo no qual deseja que os resultados sejam exibidos.

Coincidir apenas palavras inteiras - Marque essa caixa de seleção se você quiser pesquisar por palavras específicas para obter resultados mais precisos.

Diferenciar maiúsculas de minúsculas - Ative essa opção se for importante para você usar letras maiúsculas e

minúsculas na filtragem.

5.6.6.2 Localizar no log

Além da Filtragem de relatórios, é possível usar o recurso de pesquisa nos relatórios e usá-lo independente da filtragem de relatórios. Isso é útil quando você está procurando registros específicos nos relatórios. Assim como a Filtragem de relatórios, este recurso de pesquisa o ajudará a encontrar as informações que está procurando, especialmente quando há muitos registros.

Ao usar a pesquisa em relatório, é possível **Encontrar texto** ao digitar uma string específica, usar o menu suspenso **Pesquisar nas colunas** para filtrar por coluna, selecionar **Tipos de registro** e definir um **Período de tempo** para pesquisar apenas registros de um período de tempo específico. Ao especificar determinadas opções de pesquisa, apenas os registros relevantes (de acordo com as opções de filtro) serão pesquisados na janela Relatórios.

Localizar texto: Digite uma cadeia de caracteres (palavra ou parte de uma palavra). Somente os registros que contém essa cadeia de caracteres serão localizados. Outros registros serão omitidos.

Pesquisar nas colunas: - Selecione quais colunas deverão ser consideradas na pesquisa. Você pode marcar uma ou mais colunas para usar na pesquisa. Por padrão, todas as colunas estão selecionadas:

- **Hora**
- **Pasta rastreada**
- **Evento**
- **Usuário**

Tipos de objetos: Escolha um ou mais tipos de relatório de registro no menu suspenso:

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus).

Período de tempo: - Define o período de tempo no qual deseja que os resultados sejam exibidos.

- **Não especificado** (padrão) - não pesquisa no período de tempo, mas em todo o relatório.
- **Último dia**
- **Última semana**
- **Último mês**
- **Período de tempo** – você pode especificar o período de tempo exato (data e hora) para pesquisar somente os registros que ocorreram no período de tempo especificado.

Coincidir apenas palavras inteiras – Localiza apenas os registros que correspondam à cadeia de caracteres como uma palavra inteira na caixa de texto **O que**.

Diferenciar maiúsculas de minúsculas – Localiza apenas os registros que correspondam à cadeia de caracteres com maiúsculas e minúsculas exatas na caixa de texto **O que**.

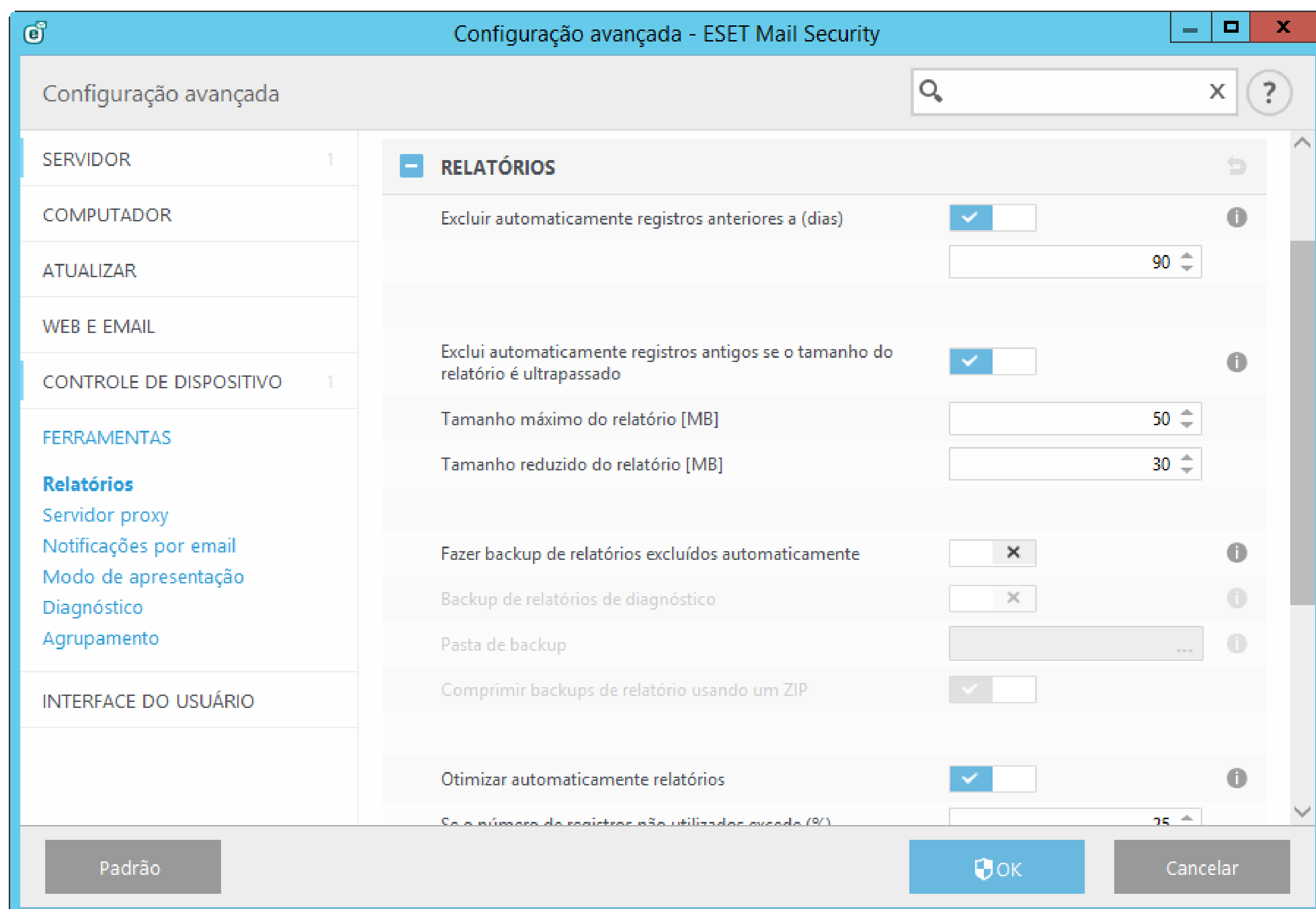
Pesquisar acima – Pesquisa da posição atual para cima.

Após configurar as opções de pesquisa, clique em **Localizar** para iniciar a pesquisa. A pesquisa pára quando encontrar o primeiro registro correspondente. Clique em **Localizar** novamente para ver registros adicionais. A pesquisa ocorre de cima para baixo nos Relatórios, começando na posição atual (registro destacado).

5.6.6.3 Manutenção de relatórios

A configuração de relatórios do ESET Mail Security pode ser acessada na janela principal do programa.

Clique em **Configuração** > **Configuração avançada** > **Ferramentas** > **Relatórios**. A seção de relatórios é utilizada para definir como os relatórios serão gerenciados. O programa exclui automaticamente os relatórios mais antigos a fim de economizar espaço no disco rígido.



- **Excluir registros automaticamente**: As entradas do relatório mais antigas que o número de dias especificado serão automaticamente excluídas.
- **Otimizar automaticamente relatórios**: Ativa a desfragmentação automática de relatórios se a porcentagem especificada de relatórios não utilizados foi excedida
- **Detalhamento mínimo de registro em relatório**: Especifica o nível de detalhamento de registro em relatório. Opções disponíveis:
  - **Registros de diagnóstico** - Registra as informações necessárias para ajustar o programa e todos os registros mencionados anteriormente
  - **Registros informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente
  - **Avisos** - Registra mensagens de erros críticos e de aviso
  - **Erros** – Somente as mensagens do tipo "Erro ao fazer download de arquivo" e erros críticos serão registrados
  - **Avisos críticos** – Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, etc...)

5.6.7 Servidor proxy

Em grandes redes, a conexão do seu computador com a Internet pode ser mediada por um servidor proxy. Se esse for o caso, as configurações a seguir precisarão ser definidas. Caso contrário, o programa não poderá se atualizar automaticamente. No ESET Mail Security, a configuração do servidor proxy está disponível em duas seções diferentes na árvore Configuração avançada.

As configurações do servidor proxy podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Mail Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, ative a opção **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, ative a opção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos. Clique em **Detectar** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

i **OBSERVAÇÃO:** Esse recurso não recupera dados de autenticação (nome de usuário e senha); eles devem ser fornecidos por você.

As configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização (**Configuração avançada** > **Atualizar** > **Proxy HTTP** ao selecionar **Conexão através de um servidor proxy** no menu suspenso **Modo proxy**). Essa configuração será aplicada ao perfil de atualização especificado e é recomendada para laptops que recebem frequentemente atualizações de assinatura de vírus de diferentes locais. Para obter mais informações sobre essa configuração, consulte a seção Configuração avançada de atualização.

5.6.8 Notificações por email

O ESET Mail Security poderá enviar automaticamente e-mails de notificação se um evento com o nível de detalhamento selecionado ocorrer. Ative **Enviar notificações de evento por email** para ativar notificações por e-mail.

OBSERVAÇÃO: Os servidores SMTP com criptografia TLS são compatíveis com o ESET Mail Security.

- **Servidor SMTP** - O servidor SMTP usado para o envio de notificações.
- **Nome de usuário e senha** - Se o servidor SMTP exigir autenticação, esses campos devem ser preenchidos com nome de usuário e senha válidos para conceder acesso ao servidor SMTP.

- **Endereço do remetente** - Esse campo especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação.
- **Endereço do destinatário** - Esse campo especifica o endereço do destinatário que será exibido no cabeçalho dos emails de notificação.

- **Detalhamento mínimo de notificações** - Especifica o nível de detalhamento mínimo de notificações a serem enviadas.
- **Ativar TLS** - Ativa mensagens de alerta e notificação compatíveis com a criptografia TLS.

- **Intervalo depois do qual cada novo email de notificação será enviado (min)** - Intervalo em minutos depois do qual cada nova notificação será enviada por email. Configure este valor como 0 se quiser enviar as notificações imediatamente.
- **Enviar cada notificação em um email separado** - Quando ativado, o destinatário receberá um novo email para cada notificação individual. Isso pode resultar em um grande número de emails recebidos em um curto período de tempo.

Formato de mensagem

- **Formato de mensagens de eventos** - O formato de mensagens de eventos que são exibidas em computadores remotos. Consulte também Editar formato.
- **Formato das mensagens de aviso de ameaça** - Mensagens de alerta de ameaça e notificação têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem. Consulte também Editar formato.

- **Utilizar caracteres do alfabeto local** - Converte uma mensagem de email na codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250). Se você deixar essa opção desmarcada, uma mensagem será convertida e codificada em ACSII de 7 bits (por exemplo, "á" será alterada para "a" e um símbolo desconhecido para "?").
- **Utilizar codificações de caracteres locais** - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

5.6.8.1 Formato de mensagem

As comunicações entre o programa e um usuário remoto ou administrador do sistema são feitas por meio de e-mails ou mensagens de rede local (usando o serviço de mensagens do Windows®). O formato padrão das mensagens de alerta e notificações será o ideal para a maioria das situações. Em algumas circunstâncias, você pode precisar alterar o formato de mensagens de evento.

As palavras-chave (cadeias de caractere separadas por sinais %) são substituídas na mensagem pelas informações reais conforme especificadas. As palavras-chave disponíveis são:

- **%TimeStamp%** - Data e hora do evento
- **%Scanner%** - Módulo relacionado
- **%ComputerName%** - Nome do computador no qual o alerta ocorreu
- **%ProgramName%** - Programa que gerou o alerta
- **%InfectedObject%** – Nome do arquivo, mensagem, etc. infectados
- **%VirusName%** - Identificação da infecção
- **%ErrorDescription%** -Descrição de um evento não vírus

As palavras-chave **%InfectedObject%** e **%VirusName%** são usadas somente em mensagens de alerta de ameaça, enquanto **%ErrorDescription%** é usada somente em mensagens de evento.

5.6.9 Modo de apresentação

O modo de apresentação é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Ele também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivírus. Quando ativado, todas as janelas pop-up são desativadas e tarefas agendadas não são executadas. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

Clique em **Configuração** > **Computador** e então clique na opção ao lado de **Modo de apresentação** para ativar o modo de apresentação manualmente. Na **Configuração avançada** (F5), clique em **Ferramentas** > **Modo de apresentação** e clique na opção ao lado de **Ativar automaticamente o modo de apresentação ao executar aplicativos em tela cheia** para que o ESET Mail Security ative o modo de apresentação automaticamente quando aplicativos em tela cheia forem executados. Ativar automaticamente o modo de apresentação é um risco de segurança em potencial, pois o ícone do status da proteção na barra de tarefas ficará laranja e exibirá um aviso. Esse aviso também pode ser visto na janela do programa principal, onde a opção **Modo de apresentação ativado** será exibida em laranja.

Quando a opção **Ativar automaticamente o modo de apresentação ao executar aplicativos em tela cheia** for marcada, o modo de apresentação será iniciado depois que você iniciar um aplicativo em tela cheia e será interrompido automaticamente ao sair do aplicativo. Esse recurso é especialmente útil para iniciar o modo de apresentação logo após iniciar um jogo, abrir um aplicativo em tela cheia ou iniciar uma apresentação.

Você também pode selecionar **Desativar o modo de apresentação automaticamente após** para definir o período de tempo em minutos após o qual o modo de apresentação será desativado automaticamente.

5.6.10 Diagnóstico

O diagnóstico fornece despejos de memória de aplicativos dos processos da ESET (por exemplo, *ekrn*). Se um aplicativo falhar, um despejo será gerado. Isso poderá ajudar os desenvolvedores a depurar e a corrigir os problemas do ESET Mail Security. Clique no menu suspenso ao lado de **Tipo de despejo** e selecione uma das três opções disponíveis:

- Selecione **Desativar** (padrão) para desativar esse recurso.
- **Mini** - Registra o menor conjunto de informações úteis que podem ajudar a identificar porque o aplicativo parou inesperadamente. Esse tipo de arquivo de despejo pode ser útil quando o espaço é limitado. No entanto, devido às informações limitadas incluídas, os erros que não foram causados diretamente pelo encadeamento que estava em execução no momento em que o problema ocorreu, podem não ser descobertos por uma análise desse arquivo.
- **Completo** - Registra todo o conteúdo da memória do sistema quando o aplicativo para inesperadamente. Um despejo de memória completo pode conter dados de processos que estavam em execução quando o despejo de memória foi coletado.

Diretório de destino – Diretório no qual o despejo durante a falha será gerado.

Abrir pasta de diagnóstico - Clique em **Abrir** para abrir esse diretório em uma nova janela do *Windows explorer*.

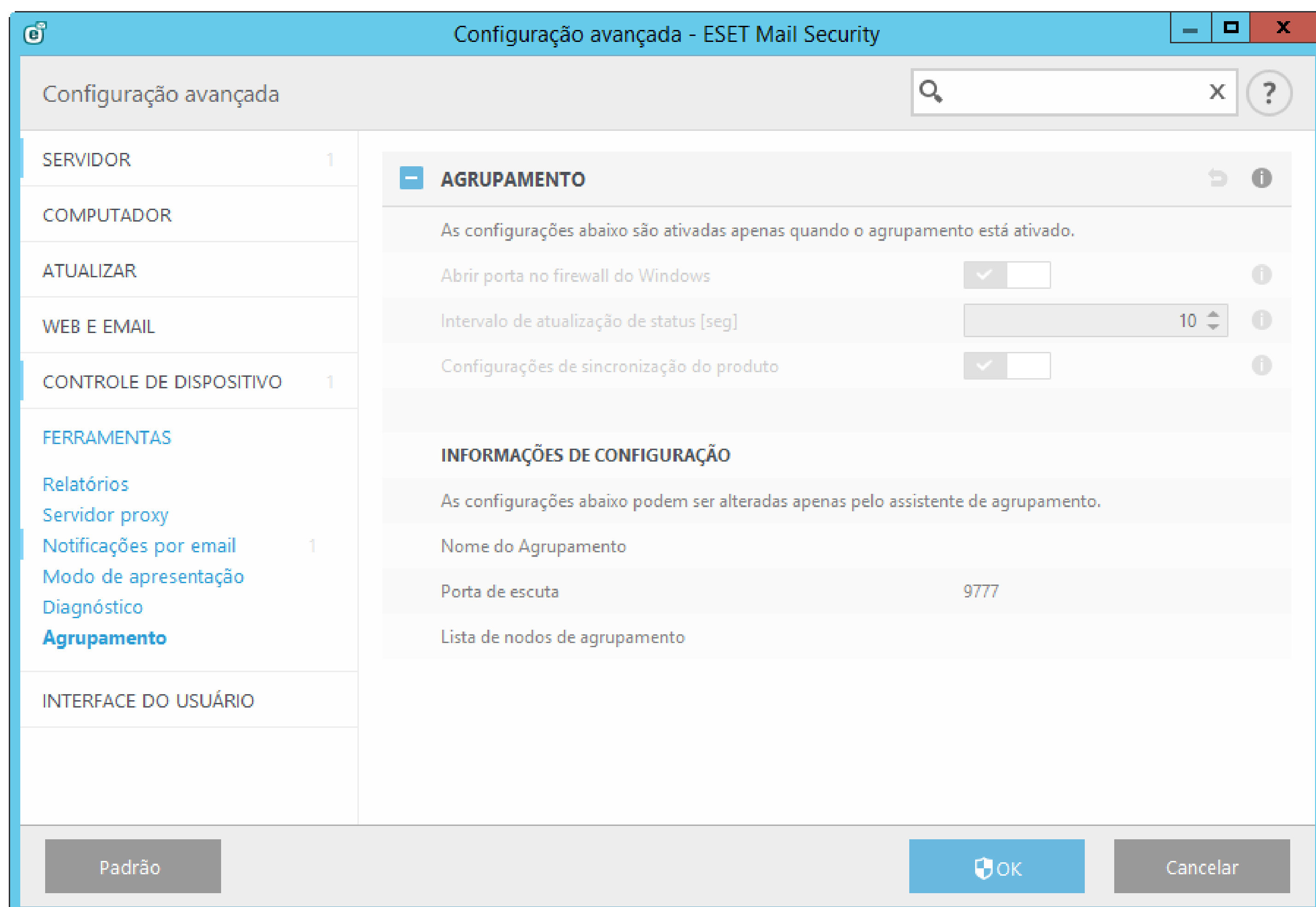
5.6.11 Atendimento ao Cliente

Enviar dados de configuração do sistema - Selecione **Sempre enviar** no menu suspenso, ou selecione **Perguntar antes de enviar** para ser consultado antes de enviar os dados.

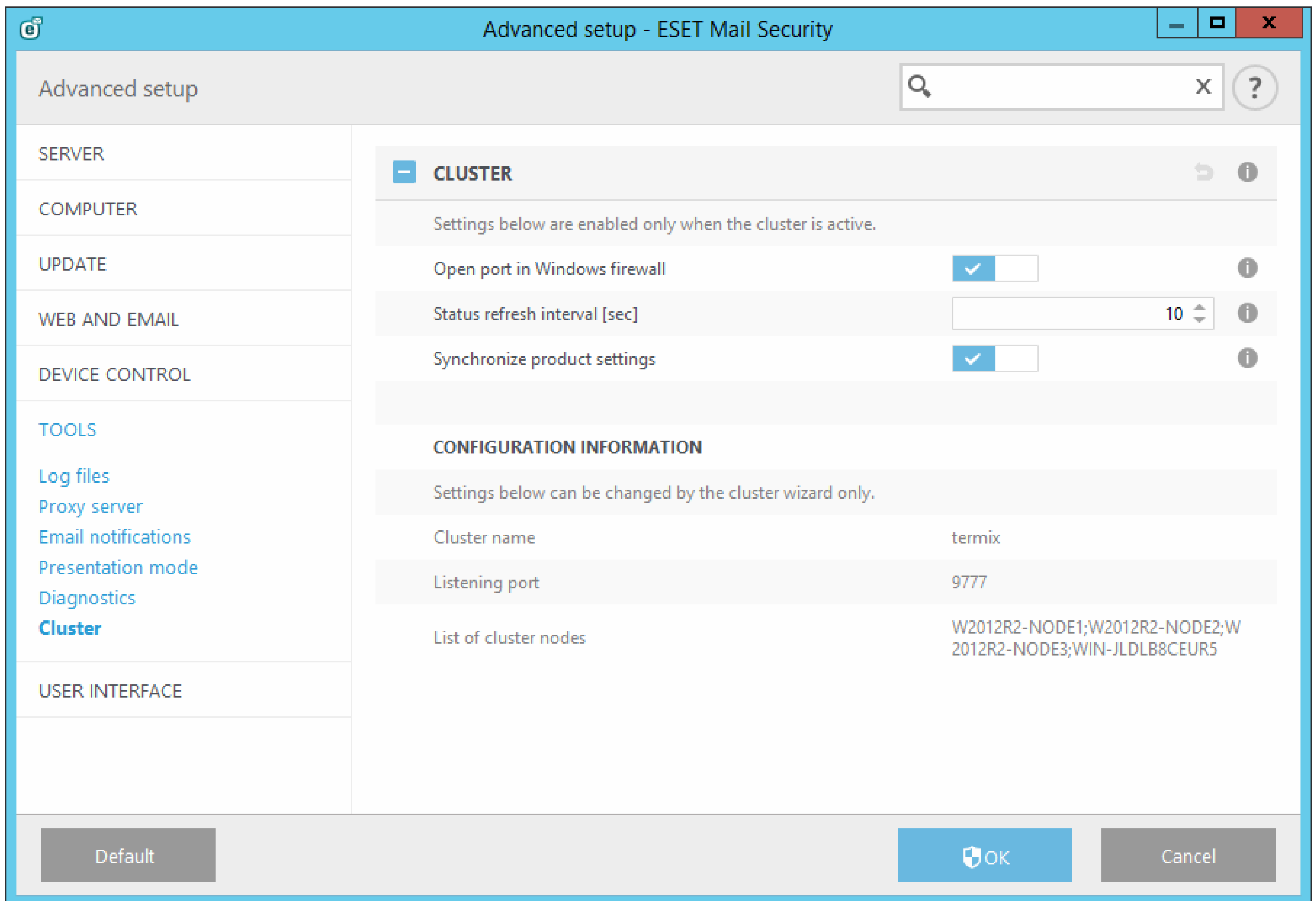
5.6.12 Agrupamento

Ativar Agrupamento é ativado automaticamente quando o Agrupamento ESET está configurado. Ela pode ser desativada manualmente na janela de Configuração avançada ao clicar no ícone de interruptor (isto é adequado para quando quiser alterar a configuração sem afetar os outros nós no Agrupamento ESET). A opção apenas ativa ou desativa a funcionalidade do Agrupamento ESET. Para configurar ou destruir adequadamente o agrupamento é necessário usar o assistente de agrupamento ou Destruir agrupamento localizado na seção **Ferramentas** > **Agrupamento** da janela principal do programa.

Agrupamento ESET não configurado e desativado:



Agrupamento ESET configurado adequadamente com seus detalhes e opções:



Para mais informações sobre o Agrupamento ESET, clique aqui.

5.7 Interface do usuário

A seção **Interface do usuário** permite configurar o comportamento da GUI (Graphical User Interface, interface gráfica do usuário) do programa. É possível ajustar a aparência visual do programa e os efeitos.

Para obter a máxima segurança do seu software de segurança, você pode evitar quaisquer alterações não autorizadas usando a ferramenta Configuração de acesso.

Ao configurar Alertas e notificações, você pode alterar o comportamento de alertas de ameaças detectadas e notificações do sistema. Esses recursos podem ser personalizados de acordo com suas necessidades.

Se você escolher não exibir algumas notificações, elas serão exibidas na área Mensagens e status desativados. Aqui é possível verificar o status dessas notificações, mostrar mais detalhes ou removê-las dessa janela.

A Integração do menu de contexto é exibida após um clique com o botão direito do mouse no objeto selecionado. Utilize essa ferramenta para integrar os elementos de controle do ESET Mail Security no menu de contexto.

O Modo de apresentação é útil para usuários que pretendem trabalhar com um aplicativo, sem serem interrompidos por janelas pop-up, tarefas agendadas ou quaisquer componentes que possam estressar os recursos do sistema.

Elementos da interface do usuário

As opções de configuração da interface do usuário no ESET Mail Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário** > **Elementos da interface do usuário** da árvore Configuração avançada do ESET Mail Security.

Na seção **Elementos da interface do usuário**, é possível ajustar o ambiente de trabalho. A interface do usuário deve ser definida como **Terminal** se os elementos gráficos reduzirem o desempenho do seu computador ou provocarem

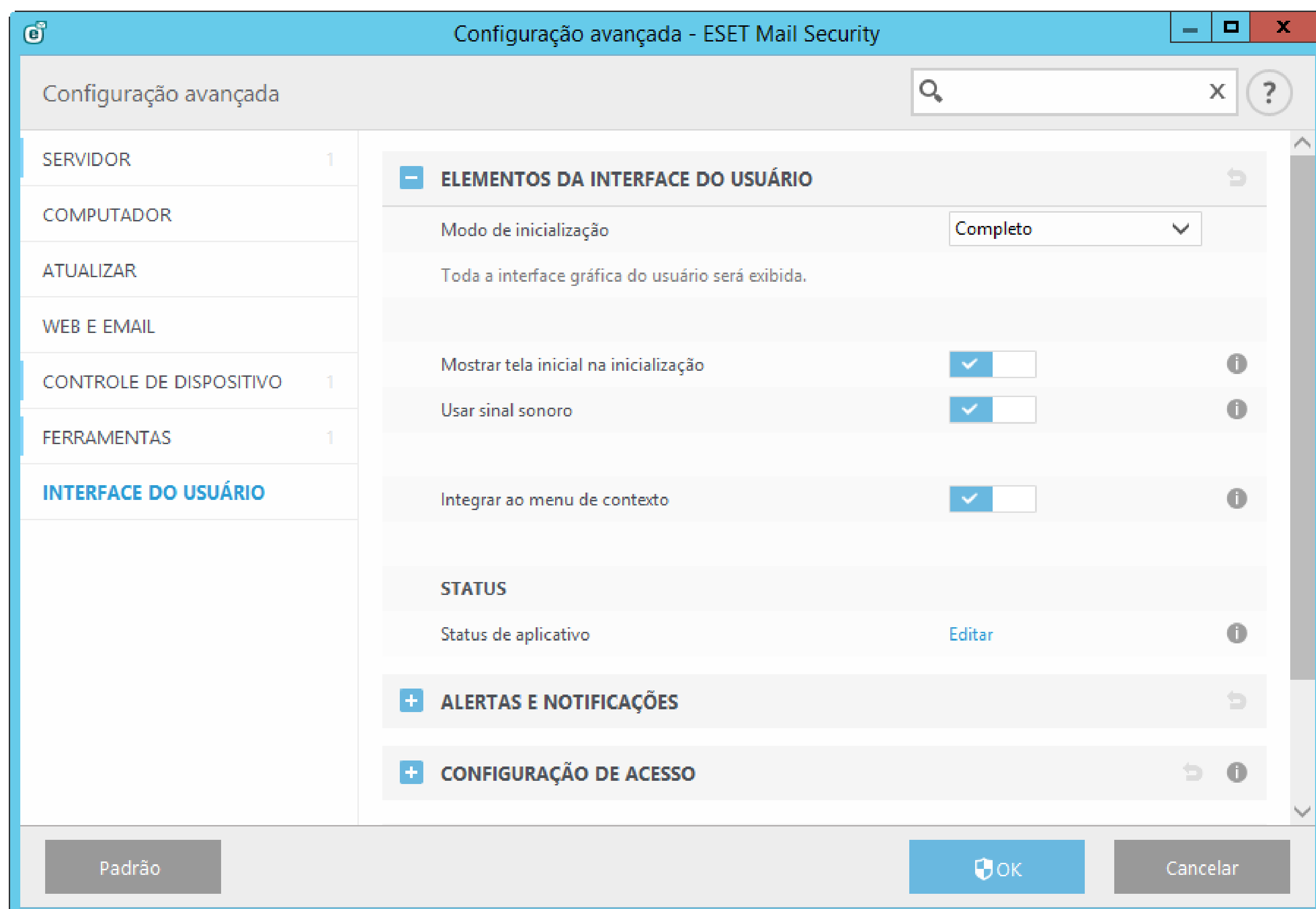
outros problemas. Você também pode querer desligar a interface gráfica do usuário em um servidor de terminal. Para mais informações sobre o ESET Mail Security instalado no servidor de terminais, consulte o tópico Desativar a interface gráfica do usuário no servidor de terminal.

Clique no menu suspenso **Modo de início de GUI** para selecionar entre os seguintes modos de início da interface gráfica do usuário:
Completo - Toda a interface gráfica do usuário será exibida.
Terminal - Nenhuma notificação ou alerta será exibido. A interface gráfica do usuário só pode ser iniciada pelo Administrador.

Se desejar desativar a tela inicial do ESET Mail Security, desmarque a opção **Mostrar tela inicial na inicialização**.

Se você quiser que o ESET Mail Security reproduza um som quando ocorrerem eventos importantes durante um rastreamento, por exemplo quando uma ameaça é descoberta ou quando a verificação for concluída, selecione **Usar sinal sonoro**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Mail Security no menu de contexto.



Status - Clique em **Editar** para gerenciar (ativar ou desativar) status que são exibidos no painel Monitoramento no menu principal.

Status de aplicativo - Permite ativar ou desativar o status de exibição no painel **Status da proteção** do menu principal.

5.7.1 Alertas e notificações

A seção **Alertas e notificações** em **Interface do usuário** permite que você configure como os alertas de ameaças e as notificações do sistema (por exemplo, mensagens de atualização bem-sucedida) são tratados no ESET Mail Security. Você também pode definir a hora e o nível de transparência das notificações da bandeja do sistema (aplica-se somente aos sistemas compatíveis com notificações na bandeja do sistema).

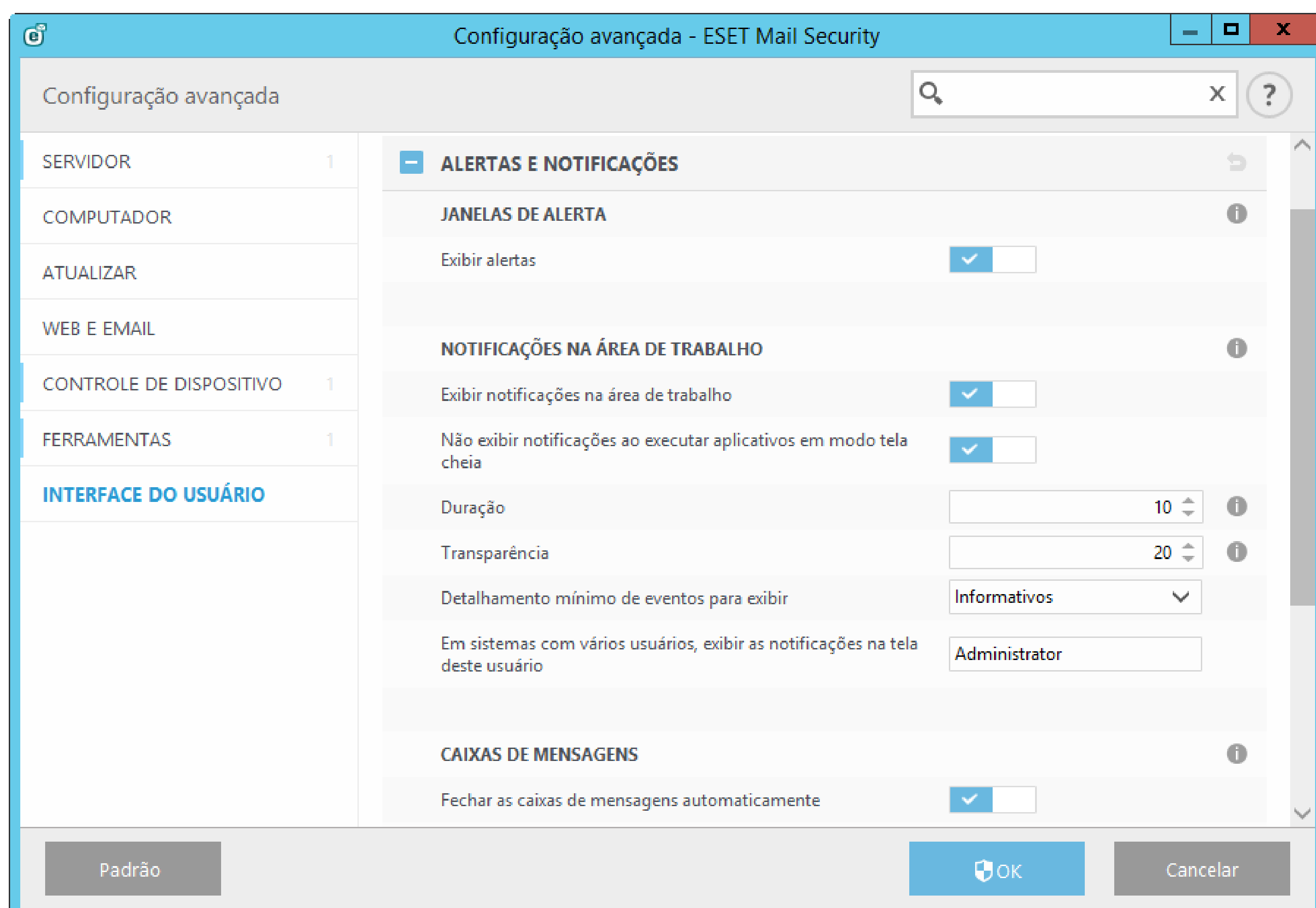
Janelas de alerta

Desativar a opção **Exibir alertas** cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Notificações na área de trabalho

As notificações na área de trabalho e as dicas de balão são apenas informativas e não requerem interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar as notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas, como o tempo de exibição e a transparência da janela de notificação, podem ser modificadas a seguir.

Ative a opção **Não exibir notificações ao executar aplicativos em modo tela cheia** para suprimir todas as notificações não interativas.



Caixas de mensagens

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o período de tempo especificado expirar.

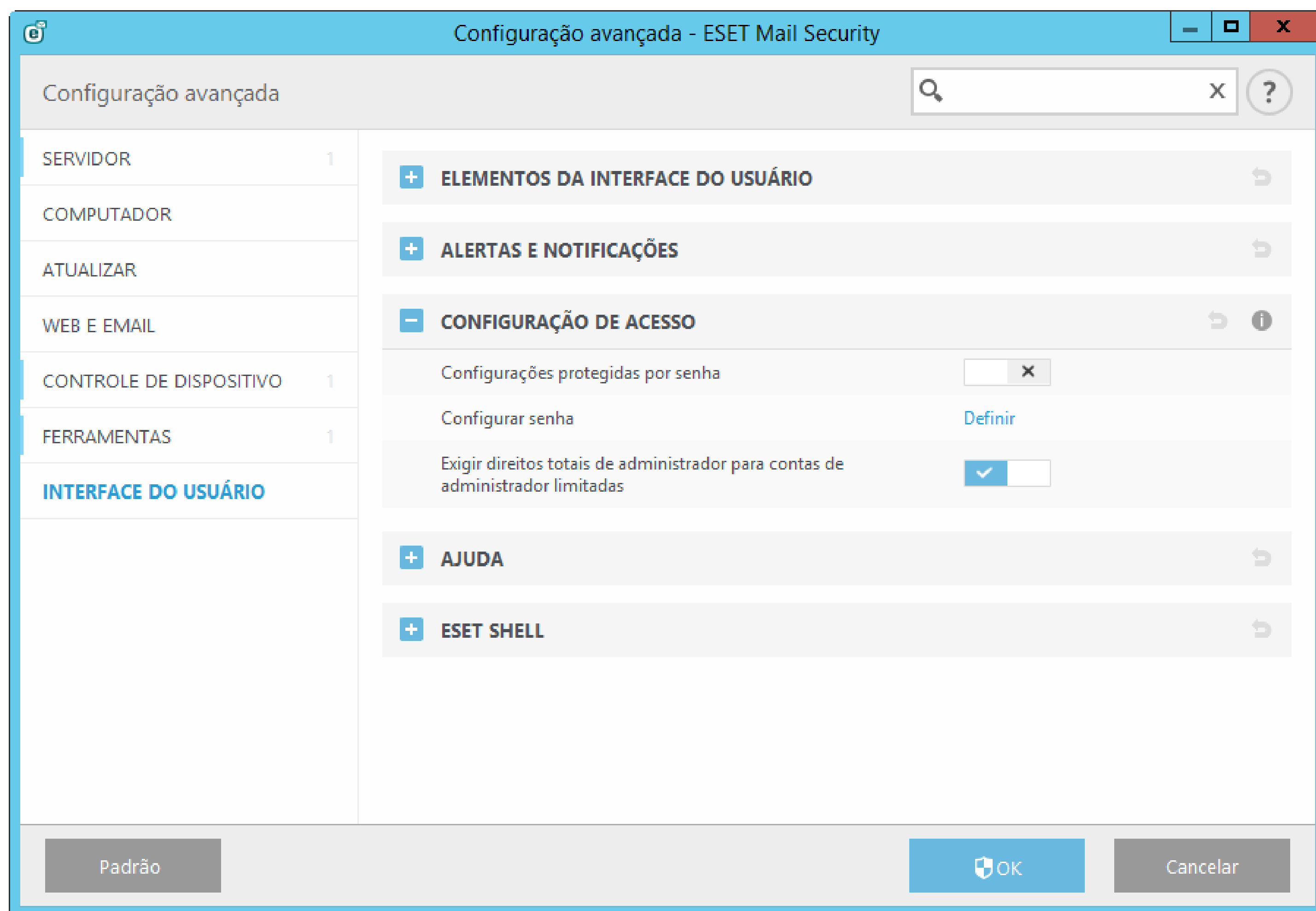
O menu suspenso **Detalhamento mínimo de eventos para exibir** permite selecionar o nível de gravidade de alertas e notificações a serem exibidos. As opções disponíveis são:

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** – Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, etc.).

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário** especifica um usuário que receberá notificações do sistema e outras notificações sobre os sistemas, permitindo que diversos usuários se conectem ao mesmo tempo. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

5.7.2 Configuração de acesso

Para fornecer segurança máxima ao seu sistema, é fundamental que o ESET Mail Security seja configurado corretamente. Qualquer alteração não qualificada pode resultar em perda de dados importantes. Para evitar modificações não autorizadas, os parâmetros de configuração do ESET Mail Security podem ser protegidos por senha. As configurações de proteção da senha estão localizadas no submenu **Configuração de acesso** em **Interface do usuário** na árvore Configuração avançada.



Configurações protegidas por senha - Bloqueia/desbloqueia os parâmetros de configuração do programa. Clique para abrir a janela Configuração de senha.

Para definir uma senha para proteger os parâmetros de configuração, clique em **Configurar senha**.

Exigir direitos totais de administrador para contas de administrador limitadas - Selecione essa opção para solicitar que o usuário atual (se ele não tiver direitos de administrador) digite o nome de usuário e a senha de administrador

quando modificar determinados parâmetros do sistema (semelhante ao UAC no Windows Vista). As alterações incluem a desativação dos módulos de proteção.

5.7.2.1 Senha

Para evitar modificação não autorizada, os parâmetros de configuração do ESET Mail Security podem ser protegidos por senha.

5.7.2.2 Configuração de senha

Para proteger os parâmetros de configuração do ESET Mail Security para evitar modificação não autorizada, uma nova senha deve ser definida. Quando quiser alterar uma senha existente, digite sua antiga senha no campo **Senha antiga**, insira sua nova senha nos campos **Nova senha** e **Confirmar senha** e clique em **OK**. Esta senha será solicitada em todas as modificações futuras que forem realizadas no ESET Mail Security.

5.7.3 Ajuda

Quando pressionar a tecla **F1** ou clicar no botão **?**, uma janela de ajuda on-line será aberta. Esta é a fonte primária de conteúdo de ajuda. Porém, também há uma cópia off-line da ajuda que vem instalada com o programa. A ajuda off-line é aberta em casos onde não há conexão com a Internet.

A versão mais recente da Ajuda on-line será exibida automaticamente quando você tiver uma conexão com a Internet.

5.7.4 ESET Shell

Você pode configurar os direitos de acesso a configurações, recursos e dados do produto através do eShell ao alterar a **Política de execução do ESET Shell**. A configuração padrão é **Script limitado**, mas ela pode ser alterada para **Desativado**, **Somente leitura** ou **Acesso completo** se necessário.

- **Desativado** - O eShell não pode ser usado. Apenas a configuração do eShell é permitida - no contexto do `ui eshell` . É possível personalizar a aparência do eShell, mas não é possível acessar qualquer configuração ou dados de produtos.
- **Somente leitura** - O eShell pode ser usado como uma ferramenta de monitoramento. Você pode exibir todas as configurações no modo Interativo e no modo de Lote, mas não pode modificar configurações, recursos ou dados.
- **Script limitado** - no modo Interativo, você pode exibir e modificar todas as configurações, recursos e dados. No Modo de lote o eShell funcionará como se estivesse no modo Somente leitura, porém se você usar arquivos em lotes assinados, será possível editar as configurações e modificar dados.
- **Acesso completo** - acesso a todas as configurações de forma ilimitada nos modos Interativo e Lote. Você pode exibir e modificar qualquer configuração. É preciso usar uma conta de administrador para executar o eShell com acesso total. Se UAC estiver ativado também é necessária uma elevação.

5.7.5 Desativar a GUI no servidor de terminal

Este capítulo descreve como desativar a interface gráfica do usuário do ESET Mail Security em execução no servidor de terminal do Windows para sessões de usuário.

Normalmente, a interface gráfica do usuário do ESET Mail Security é iniciada toda vez que um usuário remoto faz login no servidor e cria uma sessão de terminal. Isso geralmente é indesejável em servidores de terminal. Se deseja desativar a interface gráfica do usuário para sessões de terminal, isso pode ser feito no eShell executando o comando `definir ui ui gui-start-mode terminal`. Isto irá colocar a interface gráfica do usuário no modo terminal. Estes são os dois modos disponíveis para inicialização da interface gráfica do usuário:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

Se quiser descobrir qual modo é usado atualmente, execute o comando `get ui ui gui-start-mode`.

OBSERVAÇÃO: Caso tenha instalado o ESET Mail Security em um servidor Citrix, recomendamos que você use as

configurações descritas em nosso artigo da base de conhecimento.

5.7.6 Mensagens e status desativados

Mensagens de confirmação - Mostra a você uma lista de mensagens de confirmação que você pode selecionar para serem exibidas ou não.

Status de aplicativo desativado - Permite ativar ou desativar o status de exibição no painel do **Status da proteção** do menu principal.

5.7.6.1 Mensagens de confirmação

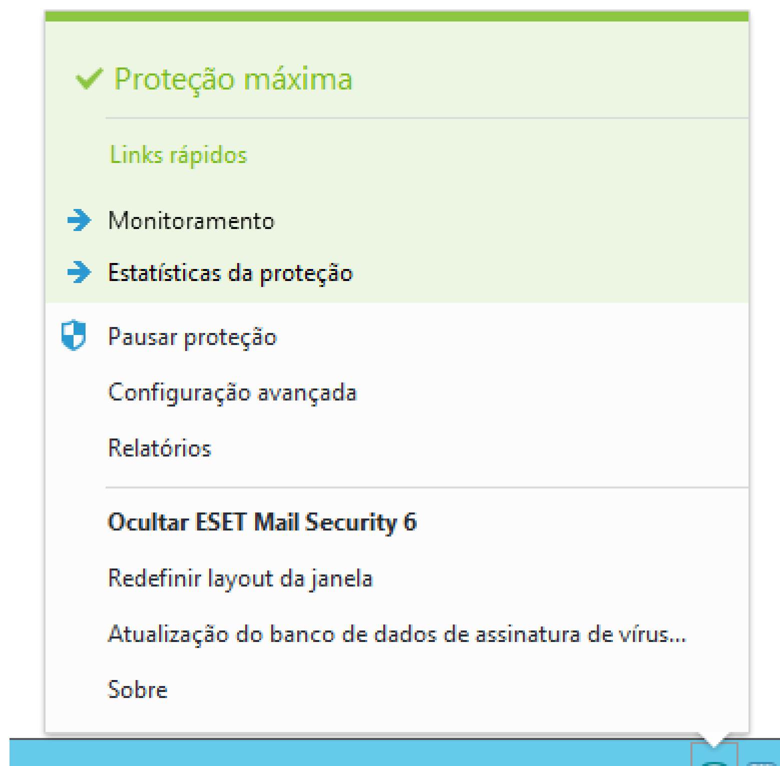
Esta janela de diálogo exibe mensagens de confirmação que o ESET Mail Security exibirá antes de qualquer ação ser realizada. Marque ou desmarque a caixa de seleção ao lado de cada mensagem de confirmação para permiti-la ou desativá-la.

5.7.6.2 Status de aplicativo desativado

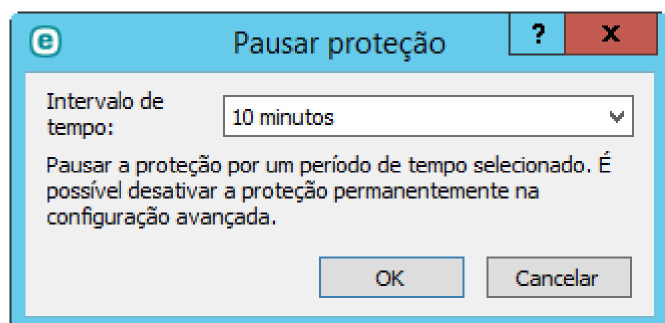
Nesta janela de diálogo, é possível marcar ou desmarcar quais status de aplicativos serão ou não exibidos. Por exemplo, quando você pausar a Proteção antivírus e antispyware ou quando ativar o Modo de apresentação. Um status de aplicativo também será exibido se seu produto não estiver ativado ou se sua licença tiver expirado.

5.7.7 Ícone da bandeja do sistema

Estão disponíveis alguns dos recursos e opções de configuração mais importantes clicando com o botão direito do mouse no ícone da bandeja do sistema .



Pausar proteção - Exibe a caixa de diálogo de confirmação que desativa a Proteção antivírus e antispyware, que protege contra ataques controlando arquivos e a comunicação via web e por emails.



O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção antivírus e antispyware será desativada.

Configuração avançada - Selecione essa opção para acessar a árvore **Configuração avançada**. Você também pode acessar a Configuração avançada pressionando a tecla F5 ou acessando **Configuração** > **Configuração avançada**.

Relatórios - Os relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas.

Ocultar ESET Mail Security - Oculta a janela do ESET Mail Security da tela.

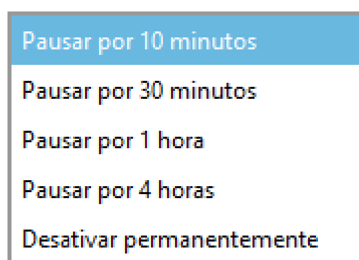
Redefinir layout da janela - Redefine a janela do ESET Mail Security para seu tamanho e posição padrão na tela.

Atualização do banco de dados de assinatura de vírus - Inicia a atualização do banco de dados de assinatura de vírus para garantir seu nível de proteção em relação ao código malicioso.

Sobre - As informações do sistema fornecem detalhes sobre a versão instalada do ESET Mail Security e os componentes do programa instalados, bem como a data de expiração de sua licença. Informações sobre seu sistema operacional e recursos do sistema podem ser encontradas no final da página.

5.7.7.1 Pausar proteção

A qualquer momento onde a Proteção antivírus e antispyware for pausada temporariamente no ícone da bandeja do sistema, a caixa de diálogo **Proteção de pausa temporária** será exibida. Isto vai desativar a proteção relacionada com malware para o período de tempo selecionado (para desativar a proteção permanentemente, é preciso usar a Configuração avançada). Tenha cuidado, desativar a proteção pode expor seu sistema a ameaças.

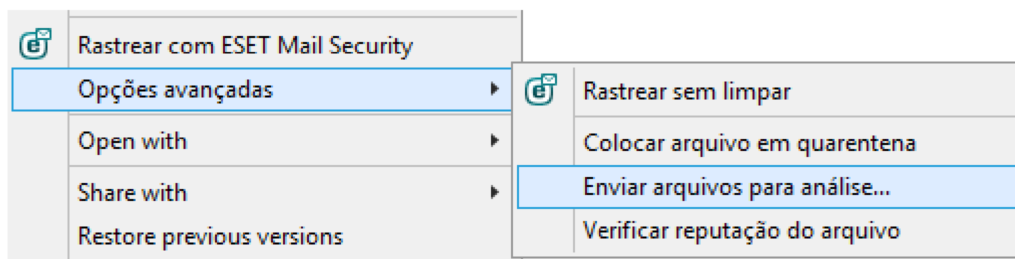


5.7.8 Menu de contexto

O menu de contexto é exibido após um clique com o botão direito do mouse em um objeto (arquivo). O menu relaciona todas as ações que você pode realizar em um objeto.

É possível integrar os elementos de controle do ESET Mail Security no menu de contexto. A opção de configuração está disponível para essa funcionalidade na árvore Configuração avançada em **Interface do usuário** > **Elementos da interface do usuário**.

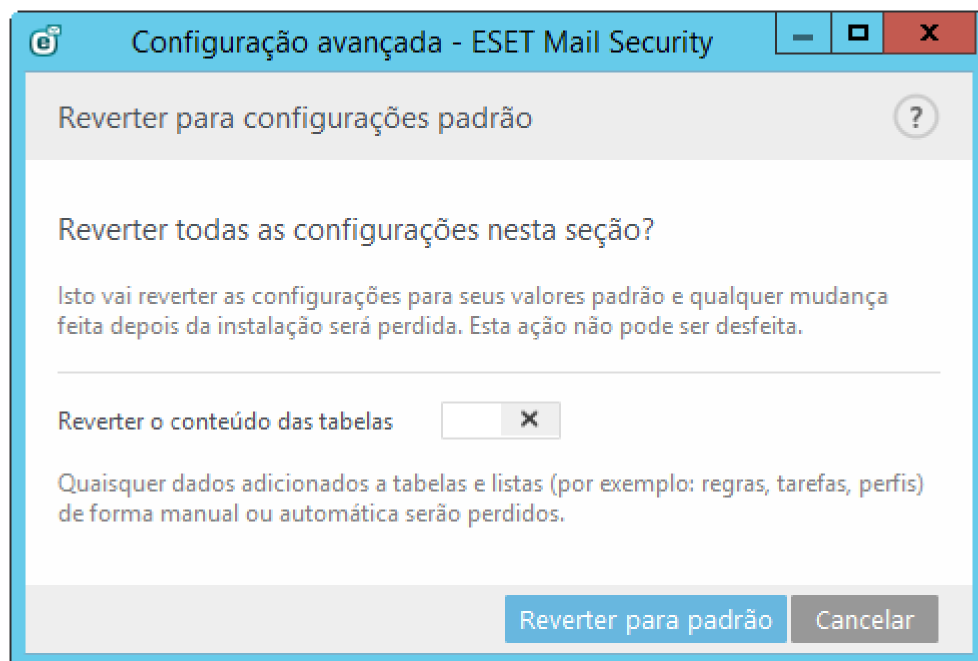
Integrar ao menu de contexto - Integra os elementos de controle do ESET Mail Security no menu de contexto.



5.8 Reverter todas as configurações nesta seção

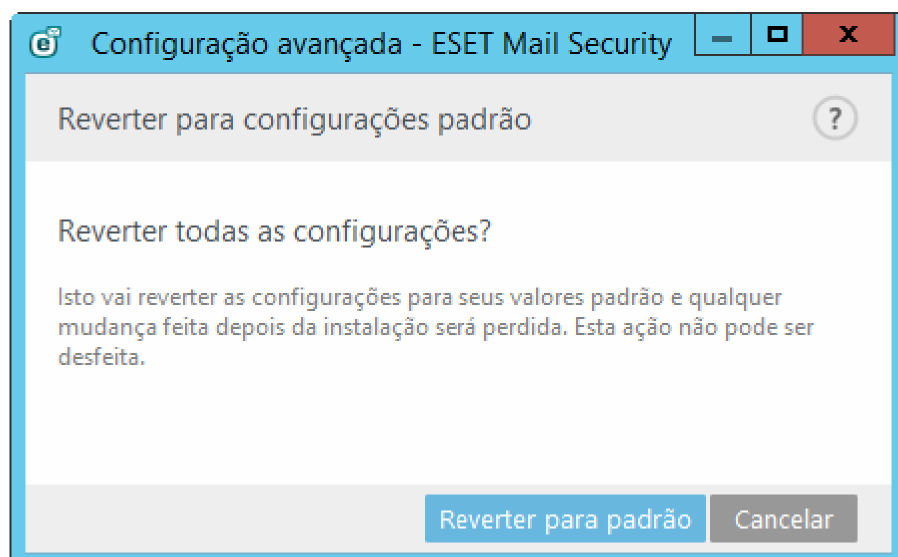
Reverte as configurações personalizadas do módulo para as configurações padrão definidas pela ESET. Observe que quaisquer alterações feitas serão perdidas depois que você clicar em **Reverter para padrão**.

Reverter conteúdo de tabelas - Quando essa opção for ativada, as regras, tarefas ou perfis adicionados manualmente ou automaticamente serão perdidos.



5.9 Reverter para configurações padrão

Todas as configurações do programa, para todos os módulos, serão redefinidos para o status que deveriam estar após uma nova instalação.



5.10 Agenda

A **Agenda** pode ser encontrada no menu principal do ESET Mail Security em **Ferramentas**. A Agenda contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção dos relatórios**
- **Atualização automática de rotina**
- **Atualizar automaticamente após conexão dial-up**
- **Atualizar automaticamente após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema (após logon do usuário)**
- **Rastreamento de arquivos em execução durante inicialização do sistema (após atualização bem sucedida do banco de dados de assinatura de vírus)**
- **Primeiro rastreamento automático**

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

5.10.1 Detalhes da tarefa

Insira o nome da tarefa e selecione uma na opção **Tipo de tarefa** e clique em **Avançar**:

- **Executar aplicativo externo**
- **Manutenção dos relatórios**
- **Rastrear arquivos na inicialização do sistema**
- **Criar um snapshot do status do computador**
- **Rastreamento sob demanda do computador**
- **Primeiro rastreamento**
- **Atualizar**

Execução de tarefas - A tarefa especificada será realizada uma vez somente na data e hora especificadas.

Uma tarefa pode ser ignorada se o computador estiver desligado ou sendo executado na bateria. Selecione quando a tarefa deve ser executada a partir de uma dessas opções e clique em **Avançar**:

- Na próxima hora agendada
- O mais breve possível
- Imediatamente, se o tempo depois da última execução ultrapassar um valor específico (horas)

5.10.2 Tempo da tarefa - único

Execução de tarefas - A tarefa especificada será realizada uma vez somente na data e hora especificadas.

5.10.3 Tempo da tarefa

A tarefa será realizada repetidamente no intervalo de tempo especificado. Selecione uma das opções de intervalo de tempo:

- **Uma vez** - A tarefa será realizada somente uma vez, na data e hora predefinidas.
- **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado (em horas).
- **Diariamente** - A tarefa será realizada diariamente na hora especificada.
- **Semanalmente** - A tarefa será realizada uma ou mais vezes por semana, no(s) dia(s) e hora selecionados.
- **Evento disparado** - A tarefa será realizada após um evento especificado.

Pular tarefa quando estiver executando na bateria - Uma tarefa não será iniciada se o computador estiver utilizando bateria no momento que a tarefa deveria ser iniciada. Isso também se aplica a computadores que são executados em UPS.

5.10.4 Tempo da tarefa - diariamente

A tarefa será executada repetidamente todos os dias no horário especificado.

5.10.5 Tempo da tarefa - semanalmente

A tarefa será executada na data e hora selecionadas.

5.10.6 Tempo da tarefa - disparado por evento

A tarefa pode ser acionada por qualquer um dos seguintes eventos:

- **Sempre que o computador for iniciado**
- **Na primeira vez em que o computador for iniciado diariamente**
- **Conexão dial-up com a Internet/VPN**
- **Na atualização bem-sucedida da base de dados das assinaturas de vírus**
- **Na atualização bem-sucedida dos componentes do programa**
- **Após logon do usuário**
- **Detecção de ameaças**

Ao agendar uma tarefa acionada por um evento, você pode especificar o intervalo mínimo entre as duas conclusões

da tarefa. Por exemplo, se você fizer logon no seu computador várias vezes ao dia, escolha 24 horas para realizar a tarefa somente no primeiro logon do dia e, em seguida, no dia seguinte.

5.10.7 Detalhes da tarefa - executar aplicativo

Essa guia agenda a execução de um aplicativo externo.

- **Arquivo executável** - Escolha um arquivo executável na árvore de diretórios, clique na opção **...** ou insira o caminho manualmente.
- **Pasta de trabalho** - Defina o diretório de trabalho do aplicativo externo. Todos os arquivos temporários do **arquivo executável** selecionado serão criados neste diretório.
- **Parâmetros** - Parâmetros da linha de comando do aplicativo (opcional).

Clique em **Concluir** para aplicar a tarefa.

5.10.8 Tarefa pulada

Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada:

- **Na próxima hora agendada** - A tarefa será executada no período especificado (por exemplo, após 24 horas).
- **Tão logo quanto possível** - A tarefa será executada assim que for possível - quando as ações que evitam a tarefa de execução não forem mais válidas.
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** - **Tempo depois da última execução (horas)** - Depois de selecionar essa opção, a tarefa será sempre executada repetidamente depois do intervalo especificado (em horas).

5.10.9 Detalhes da tarefa da agenda

Esta janela de diálogo exibe informações detalhadas sobre a tarefa agendada selecionada quando você clicar duas vezes em uma tarefa personalizada ou clicar com o botão direito do mouse em uma tarefa da agenda personalizada e clicar em **Mostrar detalhes da tarefa**.

5.10.10 Atualizar perfis

Se você desejar atualizar o programa a partir de dois servidores de atualização, é necessário criar dois perfis de atualização diferentes. Se o primeiro falhar em fazer download dos arquivos de atualização, o programa alterna para o outro. Isso é útil para notebooks por exemplo, os quais normalmente são atualizados de um servidor de atualização de rede local, mas seus proprietários frequentemente conectam-se à Internet usando outras redes. Portanto, se o primeiro perfil falhar, o segundo automaticamente fará download dos arquivos de atualização dos servidores de atualização da ESET.

Você encontrará mais informações sobre perfis de atualização no capítulo Atualização.

5.10.11 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar tarefa** ou clique com o botão direito do mouse e selecione **Adicionar** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de relatórios** - Os relatórios também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos relatórios para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um snapshot do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastreamento do computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, nós explicaremos como adicionar uma nova tarefa de atualização.

Insira o nome da tarefa no campo **Nome da tarefa**. No menu suspenso **Tipo da** tarefa selecione **Atualizar** e clique em **Avançar**.
Ative o **Ativado** se quiser ativar a tarefa (você pode fazer isso posteriormente marcando/desmarcando a caixa de seleção na lista de tarefas agendadas), clique em **Avançar** e selecione uma das opções de tempo:
Uma vez, **Repetidamente**, **Diariamente**, **Semanalmente** e **Evento disparado**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você. Depois defina a ação a ser adotada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem Intervalo da tarefa)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual é exibida. Clique em **Concluir** quando tiver concluído as alterações.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo. que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **Concluir** e a nova tarefa agendada será adicionada à lista de tarefas agendadas.

5.11 Quarentena

A principal função da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Mail Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de vírus da ESET para análise.

eset MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
MONITORAMENTO
RELATÓRIOS
RASTREAR
QUARENTENA DE EMAIL
ATUALIZAR
CONFIGURAÇÃO
FERRAMENTAS
AJUDA E SUPORTE
ENJOY SAFER TECHNOLOGY™
Quarentena

Hora	Nome do objeto	Tamanho	Motivo	Qu...
8/26/2015 9:53...	C:\Users\Administrator\AppData\Local\Mi...	184 B	Eicar arquivo de teste	1
8/26/2015 9:53...	http://www.eicar.org/download/eicar.com...	68 B	Eicar test file	7
8/25/2015 2:41...	C:\Users\Administrator\AppData\Local\Mi...	184 B	Eicar testovací súbor	1
6/1/2015 2:09:...	C:\Users\Administrator\AppData\Local\Mi...	68 B	Eicar test file	3
6/1/2015 2:09:...	C:\Users\Administrator\AppData\Local\Mi...	308 B	Eicar test file	1

Mover para quarentena... Restaurar

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, objeto adicionado pelo usuário) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças).

Colocação de arquivos em quarentena

o ESET Mail Security coloca automaticamente os arquivos excluídos em quarentena (se você não desativou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena.** O arquivo em quarentena será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena**.

Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Para isso, utilize o recurso **Restaurar**, que está disponível no menu de contexto, clicando com o botão direito do mouse no arquivo desejado, na janela Quarentena. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, a opção **Restaurar e excluir do rastreamento** estará disponível. Leia mais sobre esse tipo de aplicativo no glossário. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

i **OBSERVAÇÃO:** Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de vírus da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

5.11.1 Colocação de arquivos em quarentena

o ESET Mail Security coloca automaticamente os arquivos excluídos em quarentena (se você não desativou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena**. Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena**.

5.11.2 Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Para restaurar um arquivo na quarentena, clique com o botão direito na janela Quarentena e selecione **Restaurar** no menu de contexto. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, **Restaurar e excluir do rastreamento** também estará disponível. O menu de contexto também contém a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

Excluindo da quarentena - Clique com o botão direito em um determinado item e selecione **Excluir da quarentena**, ou selecione o item que você quer excluir e pressione **Excluir** no seu teclado. Também é possível selecionar vários itens e excluí-los juntos.

i **OBSERVAÇÃO**: Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

5.11.3 Envio de arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de ameaças da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

5.12 Atualizações do sistema operacional

A janela Atualizações do sistema mostra a lista de atualizações disponíveis prontas para serem obtidas por download e instaladas. O nível de prioridade da atualização é mostrado próximo ao nome da atualização.

Clique em **Executar atualização do sistema** para iniciar o download e a instalação de atualizações do sistema operacional.

Clique com o botão direito do mouse em uma linha para atualização e clique em **Mostrar informações** para exibir uma janela pop-up com informações adicionais.

6. Glossário

6.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

6.1.1 Vírus

Um vírus de computador é uma infiltração que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente depois disso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que o usuário, acidental ou deliberadamente, execute ou abra ele mesmo o programa malicioso.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositadamente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus (quando comparados a cavalos de troia ou spyware) estão se tornando cada vez mais raros, uma vez que eles não são comercialmente atrativos para os autores de softwares maliciosos. Além disso, o termo "vírus" é frequentemente usado de maneira incorreta para cobrir todos os tipos de infiltrações. Essa utilização está gradualmente sendo superada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador estiver infectado por um vírus, será necessário restaurar os arquivos infectados para o seu estado original, ou seja, limpá-los usando um programa antivírus.

Os exemplos de vírus são: OneHalf, Tenga e Yankee Doodle.

6.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms são propagados por meio dos endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de algumas horas após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Exemplos de worms bem conhecidos são: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

6.1.3 Cavalos de troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de infiltração que tentam se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Mas é importante observar que isso era verdadeiro para os cavalos de troia do passado, hoje não há necessidade para que eles se disfarcem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não se encaixe em uma classe específica de infiltração.

Uma vez que essa é uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** - um programa malicioso com a capacidade de fazer o download de outras infiltrações da Internet
- **Dropper** - um tipo de cavalo de troia projetado para instalar outros tipos de malware em computadores comprometidos
- **Backdoor** - um aplicativo que se comunica com agressores remotos, permitindo que eles obtenham acesso a um sistema e assumam o controle dele
- **Keylogger** - (keystroke logger) - um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos
- **Dialer** - dialers são programas projetados para se conectar aos números premium-rate. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente

Os cavalos de troia geralmente tomam a forma de arquivos executáveis com extensão .exe. Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele quase sempre contém códigos maliciosos.

Os exemplos dos cavalos de troia bem conhecidos são: NetBus, Trojandownloader. Small.ZL, Slapper.

6.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows, etc. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

1) Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
2) Quando eles estão ocultos para os testes usuais. Os usuários do ESET Mail Security têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

6.1.5 Adware

Adware é abreviação de “advertising-supported software” (software de propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage do navegador. O adware é frequentemente vinculado a programas freeware, permitindo que seus criadores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso - os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo

e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

6.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

6.1.7 Empacotadores

Empacotador é um executável de extração automática do tempo de execução que combina vários tipos de malware em um único pacote.

Os empacotadores mais comuns são UPX, PE_Compact, PKLite e ASPack. O mesmo malware pode ser detectado de forma diferente quando compactado usando outro empacotador. Empacotadores também têm a capacidade de tornar suas "assinaturas" mutáveis ao longo do tempo, tornando o malware mais difícil de ser detectado e removido.

6.1.8 Bloqueio de Exploit

O Bloqueio de Exploit é feito para fortalecer aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email ou componentes do MS Office. Ele monitora o comportamento de processos em busca de atividades suspeitas que possam indicar um exploit. Ele adiciona outra camada de proteção, uma etapa mais avançada para proteção contra invasores, ao usar uma tecnologia totalmente diferente em comparação a técnicas com foco na detecção de arquivos maliciosos.

Quando o Bloqueio de Exploit identifica um processo suspeito, ele pode interromper o processo imediatamente e registrar os dados sobre a ameaça, que são enviados ao sistema de nuvem do ESET Live Grid. Estes dados poderão ser processados pelo Laboratório de Ameaças da ESET e usados para proteger melhor todos os usuários contra ameaças desconhecidas e ataques novos (de malware recém-lançado para o qual não há solução pré-configurada).

6.1.9 Rastreamento de memória avançado

O Rastreamento de memória avançado funciona junto com o Bloqueio de Exploit com o objetivo de fornecer uma melhor proteção contra malware desenvolvido para evitar a detecção por produtos antimalware através do uso de ofuscação e/ou criptografia. Em casos em que a emulação comum ou heurística podem não detectar uma ameaça, o Rastreamento de memória avançado é capaz de identificar o comportamento suspeito e rastrear ameaças conforme elas se revelam na memória do sistema. Esta solução é eficaz contra malware que ainda esteja fortemente ofuscado. Ao contrário do Bloqueio de Exploit, este é um método de pós-execução, o que significa que existe um risco de alguma atividade maliciosa possa ter sido realizada antes de uma ameaça ser detectada. Porém no caso de outras técnicas de detecção terem falhado ele oferece uma camada adicional de segurança.

6.1.10 Arquivos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET Mail Security fornece a opção de detectar tais ameaças.

Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

6.1.11 Aplicativos potencialmente indesejados

Os **aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento antes da instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- Novas janelas que você não via anteriormente (pop-ups, ads)
- Ativação e execução de processos ocultos
- Uso aumentado de recursos do sistema
- Alterações nos resultados de pesquisa
- O aplicativo comunica-se com servidores remotos

6.2 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. É flexível, rápido e direto, e teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com os altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso – malware. A inconveniência e o perigo para você aumentam pelo fato de que o custo de enviar um spam é mínimo, e os autores do spam têm muitas ferramentas para adquirir novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas para pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou na sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".

- Use emails "especializados" – por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu email
- Utilize uma solução antispam

6.2.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. Suas principais vantagens de marketing são custos mínimos e um alto nível de objetividade, e o mais importante, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por email para se comunicar de forma eficaz com os seus clientes atuais e potenciais.

Esse tipo de publicidade é legítimo, desde que o usuário esteja interessado em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Em tais casos, a publicidade por email ultrapassa o razoável e se torna spam.

A quantidade de emails não solicitados se tornou um problema e não demonstra sinais de que vá diminuir. Os autores de emails não solicitados geralmente tentam disfarçar o spam enviando-o como mensagens legítimas.

6.2.2 Hoaxes

Um hoax é uma informação falsa propagada pela Internet. Os hoaxes geralmente são enviados por email ou ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes pedem que os destinatários encaminhem as mensagens a seus contatos, perpetuando-o. Há hoaxes de celulares, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Geralmente é impossível identificar a intenção do criador.

Se você vir uma mensagem solicitando que você a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites na Internet que podem verificar se um email é legítimo. Antes de encaminhar, execute uma pesquisa na Internet sobre qualquer mensagem que você suspeita que seja um hoax.

6.2.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (p. ex. instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, empresas de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

6.2.4 Reconhecimento de fraudes em spam

Geralmente, há poucos indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam:

- O endereço do remetente não pertence a alguém da sua lista de contatos
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais: números de contas bancárias, nomes de usuário e senhas, etc.
- Está escrito em um idioma estrangeiro
- Você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é alguém confiável (consulte o fabricante do produto original)
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo "vaigra”, em vez de “viagra” etc

6.2.4.1 Permissões

No contexto das soluções antispam e dos clientes de email, as regras são as ferramentas para manipular as funções do email. Elas são constituídas por duas partes lógicas:

1) Condição (por exemplo, uma mensagem recebida de um determinado endereço)

2) Ação (por exemplo, a exclusão da mensagem, movendo-a para uma pasta especificada)

O número e a combinação de diversas regras com a solução Antispam. Essas regras servem como medidas contra spam (email não solicitado). Exemplos típicos:

- Condição: Uma mensagem recebida contém algumas palavras geralmente vistas nas mensagens de spam 2. Ação: Excluir a mensagem
- Condição: Uma mensagem recebida contém um anexo com a extensão .exe 2. Ação: Excluir o anexo e enviar a mensagem para a caixa de correio
- Condição: Uma mensagem recebida chega do seu patrão 2. Ação: Mover a mensagem para a pasta "Trabalho"

Recomendamos que você use uma combinação de regras nos programas antispam a fim de facilitar a administração e filtrar os spams com mais eficiência.

6.2.4.2 Filtro Bayesian

A filtragem de spam Bayesian é uma forma eficiente de filtragem de email usada por quase todos os produtos antispam. Ela é capaz de identificar emails não solicitados com grande precisão e pode funcionar com base em cada usuário.

A funcionalidade baseia-se no seguinte princípio: O processo de aprendizagem acontece na primeira fase. O usuário marca manualmente um número suficiente de mensagens como mensagens legítimas ou spam (normalmente 200/200). O filtro analisa as duas categorias e aprende, por exemplo, que o spam geralmente contém as palavras "rolex" ou "viagra", e as mensagens legítimas são enviadas por familiares ou de endereços na lista de contatos do usuário. Desde que haja uma quantidade suficiente de mensagens processadas, o filtro Bayesian é capaz de atribuir um "índice de spam" específico a cada mensagem, para determinar se é ou não spam.

A principal vantagem de um filtro Bayesian é a sua flexibilidade. Por exemplo, se um usuário for um biólogo, todas as mensagens de email referentes à biologia ou aos campos de estudo relacionados serão geralmente recebidas com um índice de baixa probabilidade. Se uma mensagem incluir palavras que normalmente a qualificariam como não solicitada, mas que foi enviada por alguém da lista de contatos do usuário, ela será marcada como legítima, porque os remetentes de uma lista de contatos diminuem a probabilidade geral de spam.

6.2.4.3 Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceitas, ou para os quais foi concedida permissão. O termo "lista de permissões de email" define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de email, nomes de domínio, endereços de IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço de IP não serão recebidas. Se não forem exclusivas, tais mensagens não serão excluídas, mas filtradas de algum outro modo.

Uma lista de permissões baseia-se no princípio oposto de uma lista de proibições. As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

6.2.4.4 Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições. As criadas pelos usuários em seus aplicativos antispam e as listas de proibições profissionais atualizadas com frequência, criadas por instituições especializadas e que podem ser encontradas na Internet.

É fundamental usar as listas de proibições para bloquear spams com sucesso, mas é muito difícil mantê-las, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos que use uma lista de permissões e uma de proibições para filtrar o spam com mais eficácia.

6.2.4.5 Controle pelo servidor

O controle pelo servidor é uma técnica para identificar os spams em massa com base no número de mensagens recebidas e as reações dos usuários. Cada mensagem deixa uma "impressão digital" exclusiva no servidor com base no conteúdo da mensagem. O número de ID exclusivo não informa nada sobre o conteúdo do email. Duas mensagens idênticas terão impressões digitais idênticas, enquanto mensagens diferentes terão impressões digitais diferentes.

Se uma mensagem for marcada como spam, sua impressão digital será enviada ao servidor. Se o servidor receber mais de uma impressão digital idêntica (correspondendo a uma determinada mensagem de spam), a impressão digital será armazenada no banco de dados das impressões digitais. Ao rastrear as mensagens de entrada, o programa envia as impressões digitais das mensagens ao servidor. O servidor retorna as informações sobre que impressões digitais correspondem às mensagens já marcadas pelos usuários como spam.